

Summary of Contents

	PAGE
CONTENTS	III
PREFACE	XV
OVERVIEW	
Introduction	1
Background	13
PART BY PART ANALYSIS	
PART I: Preliminary provisions	27
PART II: Information privacy principles	57
PART III: Privacy Commissioner	109
PART IV: Good reasons for refusing access to personal information	145
PART V: Procedural provisions relating to access to and correction of personal information	175
PART VI: Codes of practice and exemptions from information privacy principles	203
PART VII: Public register personal information	231
PART VIII: Complaints	267
PART IX: Proceedings of Commissioner	291
PART X: Information matching	299
PART XI: Law enforcement information	337
PART XII: Miscellaneous provisions	349
SCHEDULES	369
SUMMARY OF RECOMMENDATIONS	373
APPENDICES	
<i>A. Acknowledgments</i>	<i>389</i>
<i>B. List of submissions</i>	<i>393</i>
<i>C. Recent overseas privacy legislation</i>	<i>397</i>
<i>D. Legislative background</i>	<i>399</i>
<i>E. PCO drafting style changes</i>	<i>401</i>
<i>F. Reports to the Minister of Justice</i>	<i>403</i>
<i>G. Commissioner's functions under other statutes</i>	<i>405</i>
<i>H. Tables of equivalent provisions</i>	<i>409</i>
<i>I. List of public registers</i>	<i>413</i>
<i>J. Complaints graphs</i>	<i>415</i>

Contents

C

PARA		PAGE
	SUMMARY OF CONTENTS	I
	CONTENTS	III
	List of figures	XIV
	PREFACE	XV
	OVERVIEW	
	INTRODUCTION	
	Review processes	2
	<i>Commencement of the review</i>	2
	<i>Discussion papers</i>	2
	<i>Completion of the report</i>	3
	Themes in the report	3
	<i>Coverage of the Act</i>	4
	<i>Enhancement of individual rights</i>	4
	<i>Effectiveness of Office of the Privacy Commissioner</i>	5
	<i>Interaction with other laws</i>	6
	<i>Compliance and administration costs</i>	7
	<i>Ease of use of the Act</i>	8
	<i>“Adequate protection” in terms of the EU Directive</i>	9
	Privacy at the end of the Twentieth Century	10
	BACKGROUND	
	International context	13
	<i>Human rights origins</i>	13
	<i>Articulating privacy principles</i>	14
	<i>European Union Directive on Data Protection</i>	15
	<i>Relevance of international considerations to the review</i>	15
	Technological context	15
	<i>National and international responses to technology</i>	15
	<i>Some local technological issues</i>	16
	<i>Benefits to privacy of technology</i>	16
	<i>Relevance of technological issues to the review</i>	17
	Economic context	17
	<i>Origins of OECD interest</i>	17
	<i>Globalisation and harmonisation</i>	18
	<i>EU Directive on Data Protection</i>	19
	<i>Public sector reform</i>	19
	<i>Economic considerations in the review</i>	20
	Legislative history	20
	<i>Introduction</i>	20
	<i>The 1970s - Experimental national legislation</i>	21
	<i>The 1980s - International standard setting, local study and sectoral legislation</i>	22
	<i>The 1990s - Comprehensive privacy legislation</i>	23
	<i>Some reflections on legislative history</i>	25

PART BY PART ANALYSIS**PART I: PRELIMINARY PROVISIONS**

1.1	Introduction	27
1.2	Drafting style	27
	<i>Introduction</i>	27
	<i>General statutory format</i>	28
	<i>Parliamentary Counsel Office changes in drafting style</i>	29
	<i>Marginal notes and headings</i>	30
	<i>Section notes and endnotes</i>	32
	<i>Consolidated reprint</i>	33
	<i>Recommendations elsewhere in report</i>	33
1.3	SECTION 1 - Short title and commencement	33
	<i>Rapid commencement</i>	33
	<i>Delayed enforceability</i>	34
1.4	SECTION 2 - Interpretation	34
	Agency	35
	<i>Subparagraphs (b)(i) and (ii): Sovereign, Governor-General etc</i>	36
	<i>Subparagraph (b)(iii): House of Representatives</i>	36
	<i>Subparagraph (b)(iv): Members of Parliament</i>	37
	<i>Subparagraphs (b)(v) and (vi): Parliamentary Service Commission and Parliamentary Service</i>	39
	<i>Paragraph (b)(vii): Courts</i>	40
	<i>Subparagraph (b)(viii): Tribunals</i>	41
	<i>Subparagraph (b)(ix): Ombudsmen</i>	42
	<i>Subparagraph (b)(xiii): News media</i>	43
	Collect	46
	Correct	47
	Document	47
	Individual	48
	Information privacy principle	48
	Permanent resident of New Zealand	48
	Personal information	49
	Public register	49
	Public sector agency	49
	Publicly available information and publicly available publication	51
	Statutory officer	52
	Working day	52
	New definitions	53
	<i>Use</i>	53
	Section 2(2)	55
1.5	SECTION 3 - Information held by agency	55
1.6	SECTION 4 - Actions of, and disclosure of information to, staff of agency, etc	55
1.7	SECTION 5 - Act to bind the Crown	56

PART II: INFORMATION PRIVACY PRINCIPLES

2.1	Introduction	57
	<i>Origins of the principles</i>	58
	<i>Principles or sections?</i>	58
2.2	SECTION 6 - Information privacy principles	59
2.3	Principle 1 - Purpose of collection of personal information	60
	<i>International origins and comparisons</i>	60
2.4	Principle 2 - Source of personal information	61
	<i>Rationale, origins and overseas comparisons</i>	61
	<i>Exceptions</i>	62
	<i>Notice to individual when collecting from another source</i>	63

2.5	Principle 3 - Collection of information from subject	64
	<i>Explanations required by principle 3(1)</i>	64
	<i>Purpose or purposes</i>	66
	<i>Principle 3(2) and (3)</i>	67
	<i>Exceptions</i>	67
	<i>Authorisation for non-compliance</i>	67
	<i>Statistical or research purposes exception</i>	67
2.6	Principle 4 - Manner of collection of personal information	70
2.7	Principle 5 - Storage and security of personal information	71
	<i>Recent international security safeguards developments</i>	71
	<i>Browsing or inspection of information</i>	73
2.8	Principle 6 - Access to personal information	74
	<i>Legislative history</i>	74
2.9	Principle 7 - Correction of personal information	75
	<i>Obligation to advise of right under principle 7(1)(b)</i>	76
	<i>Preventing use of information for purposes of direct marketing</i>	76
2.10	Principle 8 - Accuracy, etc, of personal information to be checked before use	78
	<i>Meaning of “use”</i>	79
2.11	Principle 9 - Agency not to keep personal information for longer than necessary	80
	<i>Other jurisdictions</i>	81
	<i>Other enactments</i>	81
	<i>Requirement to retain information</i>	82
2.12	Principle 10 - Limits on use of personal information	84
	<i>Exceptions</i>	84
2.13	Principle 11 - Limits on disclosure of personal information	85
	<i>Disclosure for enforcement of foreign laws</i>	86
2.14	Principle 12 - Unique identifiers	87
	<i>Rationale for principle 12</i>	88
	<i>The meaning of “assign”</i>	89
	<i>Limiting principle 12(2) to public sector unique identifiers</i>	90
	<i>Enforceability of principle 12(2)</i>	91
2.15	SECTION 7 - Savings provision	92
	<i>Subsections 7(1) to (6)</i>	93
	<i>Simplifying the savings regime</i>	93
	<i>Marginal note</i>	94
	<i>Dispersal of elements of section 7</i>	94
	<i>Sections 7(2) and (3) as they concern principle 11</i>	96
	<i>Restrictions on access in regulations</i>	98
	<i>Restrictions on access in other statutes</i>	99
	<i>The rump of section 7</i>	100
2.16	SECTION 8 - Application of information privacy principles	101
2.17	SECTION 9 - Postponement of application of principle 11 to lists used for direct marketing	101
2.18	SECTION 10 - Application of principles to information held overseas	102
	Transborder data flows	102
	<i>International approaches to transborder data flow issues</i>	103
	<i>EU Directive and transborder data flows</i>	104
	<i>Transborder data flow proposal</i>	106
2.19	SECTION 11 - Enforceability of principles	107
	<i>Private prosecutions</i>	107
PART III: PRIVACY COMMISSIONER		
3.1	Introduction	109
3.2	SECTION 12 - Privacy Commissioner	110
	<i>Officer of Parliament</i>	110

	<i>Crown entity</i>	111
3.3	SECTION 13 - Functions of Commissioner	111
	<i>Function (a): Education and publicity</i>	111
	<i>Privacy hotline</i>	112
	<i>Written enquiries</i>	112
	<i>Written publications</i>	113
	<i>Newsletter</i>	113
	<i>Privacy Issues Forum</i>	113
	<i>Case notes</i>	113
	<i>Internet</i>	114
	<i>Participation in conferences</i>	114
	<i>Co-operation with commercial publishers and journals</i>	114
	<i>Code commentary</i>	114
	<i>News media</i>	114
	<i>Function (b): Audit of personal information</i>	114
	<i>Canada</i>	115
	<i>UK and Hong Kong</i>	116
	<i>NZ auditing</i>	117
	<i>Function (c): Monitoring use of unique identifiers</i>	118
	<i>Function (d): Directories of personal information</i>	119
	<i>Function (e): Monitoring compliance with public register principles</i>	119
	<i>Function (f): Examination of proposed information matching provisions</i>	119
	<i>Function (g): Educational programmes</i>	120
	<i>Seminar series with NZ Law Society</i>	120
	<i>Seminar series with other organisations</i>	121
	<i>Seminars and workshops</i>	121
	<i>Videotape</i>	121
	<i>Private Lives? Privacy and Disability Issues</i>	121
	<i>Function (h): Public statements</i>	121
	<i>Function (i): Representations from the public</i>	122
	<i>Function (j): Co-operation with others concerned with privacy</i>	122
	<i>Regional co-operation</i>	123
	<i>International co-operation</i>	124
	<i>Other co-operation</i>	124
	<i>Function (k): Suggestions for action</i>	124
	<i>Function (l): Advice to Ministers or agencies</i>	125
	<i>Function (m): Inquiry into enactments, practices, procedures, technical developments etc</i>	125
	<i>Function (n): Research and monitoring data processing and computer technology</i>	125
	<i>Function (o): Examination of proposed legislation</i>	126
	<i>Function (p): Report to Prime Minister on need for action</i>	127
	<i>Function (q): Report to PM on acceptance of international instrument</i>	127
	<i>Function (r): Report to PM on any other matter</i>	127
	<i>Function (s): Gathering information</i>	128
	<i>Function (t): Incidental or conducive functions</i>	128
	<i>Function (u): Other enactments</i>	128
	<i>Complaints mechanisms</i>	129
	<i>Approval of, and consultation with, Commissioner</i>	129
	<i>Appointment to other bodies</i>	129
	<i>Codes of practice and information matching</i>	129
	<i>Subsection (2)</i>	130
3.4	SECTION 14 - Commissioner to have regard to certain matters	130
3.5	SECTION 15 - Deputy Commissioner	131
3.6	SECTION 16 - Term of office	132
3.7	SECTION 17 - Continuation in office after term expires	132

3.8	SECTION 18 - Vacation of office	133
3.9	SECTION 19 - Holding of other offices	133
3.10	SECTION 20 - Powers relating to declaratory judgments	133
3.11	SECTION 21 - Directories of personal information	134
	<i>Worth of directory questioned</i>	134
	<i>Directory of Official Information</i>	135
	<i>Compliance costs</i>	135
3.12	SECTION 22 - Commissioner may require agency to supply information	136
3.13	SECTION 23 - Privacy officers	137
	<i>Appointment of outside privacy officers</i>	137
	<i>Privacy officer support</i>	138
3.14	SECTION 24 - Annual report	139
3.15	SECTION 25 - Further provisions relating to Commissioner	139
	<i>First Schedule: Clause 2 - Staff</i>	140
	<i>First Schedule: Clause 6 - Services for Commissioner</i>	140
3.16	SECTION 26 - Review of operation of Act	140
	<i>Bouquets & brickbats - the review process</i>	144
PART IV: GOOD REASONS FOR REFUSING ACCESS TO PERSONAL INFORMATION		
4.1	Introduction	145
	<i>Legislative history</i>	146
	<i>Law Commission review</i>	147
	<i>Grouping of withholding grounds</i>	147
4.2	SECTION 27 - Security, defence, international relations etc.	148
	<i>Marginal note</i>	149
	27(1)(a): Security, defence, international relations	149
	27(1)(b): Inter-governmental entrusting of information	149
	27(1)(c): Maintenance of the law	150
	<i>Informant identity</i>	150
	<i>Investigation and detection of offences</i>	150
	<i>TAIC</i>	151
	<i>Canadian law enforcement provisions</i>	151
	27(1)(d): Endangering the safety of an individual	152
4.3	SECTION 28 - Trade secrets	153
	28(1)(a): Trade secrets	154
	28(1)(b): Prejudice commercial position	155
4.4	SECTION 29 - Other reasons for refusal of requests	156
	29(1)(a): Unwarranted disclosure of the affairs of another	157
	29(1)(b): Evaluative material	158
	<i>Meaning of “supply”</i>	159
	<i>Response to include grounds</i>	160
	<i>Evaluative material held by author</i>	160
	29(1)(c): Physical or mental health	161
	<i>Use of provision</i>	161
	<i>Psychologists</i>	161
	29(1)(d): Young persons	162
	29(1)(e): Safe custody or rehabilitation	163
	29(1)(f): Legal professional privilege	164
	29(1)(g): Radio NZ Ltd/TVNZ Ltd	165
	<i>Restructuring of RNZ</i>	165
	<i>Protection of sources</i>	165
	<i>Access, correction and the news media</i>	166
	29(1)(h): Library, museum or archive	167
	29(1)(i): Contempt of court or Parliament	167

	<i>29(1)(j): Frivolous, vexatious or trivial</i>	167
	<i>29(2): Unavailability of information</i>	168
	<i>29(2)(a): Not readily retrievable</i>	168
	<i>29(2)(b): Information requested does not exist or cannot be found</i>	169
	<i>29(2)(c): Requested information is not held</i>	170
	<i>29(3): Evaluative material</i>	170
4.5	SECTION 30 - Refusal not permitted for any other reason	171
	<i>Counselling and medical privileges</i>	171
4.6	SECTION 31 - Restriction when person sentenced to imprisonment	172
4.7	SECTION 32 - Information concerning existence of certain information	173
	<i>Broadening the application of section 32</i>	173
PART V: PROCEDURAL PROVISIONS RELATING TO ACCESS TO AND CORRECTION OF PERSONAL INFORMATION		
5.1	Introduction	176
5.2	SECTION 33 - Application	177
5.3	SECTION 34 - Who may make requests	177
	<i>Importance of access and correction rights</i>	177
	<i>International considerations</i>	178
	<i>Legislative history</i>	179
	<i>Practicalities concerning overseas requests</i>	180
	<i>Adoption (Intercountry) Act 1997</i>	181
	<i>Parents and children etc</i>	181
5.4	SECTION 35 - Charges	184
	<i>Charging for correction</i>	184
	<i>Misuse of access right</i>	186
	<i>Charging guidelines</i>	188
5.5	SECTION 36 - Commissioner may authorise public sector agency to charge	189
5.6	SECTION 37 - Urgency	189
	<i>Urgent cases on review</i>	191
5.7	SECTION 38 - Assistance	191
	<i>Assistance and charging</i>	192
	<i>Assistance and urgency</i>	192
5.8	SECTION 39 - Transfer of requests	192
	<i>Where individual does not want transfer</i>	192
5.9	SECTION 40 - Decisions on requests	193
	<i>What is the “time limit”?</i>	193
	<i>Subsections (3) and (4)</i>	194
5.10	SECTION 41 - Extension of time limits	195
	<i>Multiple extensions</i>	196
	<i>Grounds for extension</i>	196
	<i>Outer time limit</i>	197
	<i>“As soon as reasonably practicable”</i>	197
5.11	SECTION 42 - Documents	197
	<i>Origin and operation of provision</i>	197
	<i>Loans of documents</i>	198
5.12	SECTION 43 - Deletion of information from documents	199
5.13	SECTION 44 - Reason for refusal to be given	200
5.14	SECTION 45 - Precautions	200

PART VI: CODES OF PRACTICE AND EXEMPTIONS FROM INFORMATION PRIVACY PRINCIPLES

6.1	Introduction	203
-----	---------------------	-----

	<i>Codes and exemptions</i>	203
	<i>Legislative history</i>	204
	<i>Why codes of practice</i>	205
	<i>Role and placement of exemptions and exceptions</i>	205
6.2	SECTION 46 - Codes of practice	207
	<i>Section 46(2)(aa)</i>	208
	<i>Section 46(4)</i>	209
	<i>Section 46(6) and (7)</i>	210
6.3	SECTION 47 - Proposal for issuing code of practice	211
	<i>Representative body applications</i>	211
	<i>Costs of section 47(2) applications</i>	213
	<i>Section 47(5)</i>	213
6.4	SECTION 48 - Notification of intention to issue code	214
6.5	SECTION 49 - Notification, availability and commencement of code	215
6.6	SECTION 50 - Codes deemed to be regulations for purposes of disallowance	216
6.7	SECTION 51 - Amendment and revocation of codes	217
6.8	SECTION 52 - Urgent issue of code	217
6.9	SECTION 53 - Effect of code	218
6.10	SECTION 54 - Commissioner may authorise collection, use, or disclosure of personal information	218
	<i>Section 54</i>	219
	<i>Extension to principle 9</i>	219
	<i>Public notification costs</i>	220
6.11	SECTION 55 - Certain personal information excluded	220
	<i>Royal Commissions and commissions of inquiry</i>	221
6.12	SECTION 56 - Personal information relating to domestic affairs	222
6.13	SECTION 57 - Intelligence organisations	224
	<i>Introduction</i>	224
	<i>Existing position of intelligence organisations</i>	224
	<i>Extension of other principles to intelligence organisations</i>	225
	<i>Principle 1</i>	226
	<i>Principle 5</i>	226
	<i>Principle 8</i>	227
	<i>Principle 9</i>	227
	<i>Inspector-General of Intelligence and Security</i>	229
	PART VII: PUBLIC REGISTER PERSONAL INFORMATION	
7.1	Introduction	231
	<i>Overview</i>	231
	<i>Terminology</i>	232
	<i>Council of Europe Recommendation R(91)10</i>	232
	<i>Public register issues and risks</i>	233
	<i>Consultation</i>	234
7.2	SECTION 58 - Interpretation	235
	<i>Location of definitions</i>	235
	<i>Definition of “public register”</i>	235
	<i>Possible new definitions</i>	237
7.3	SECTION 59 - Public register privacy principles	237
7.4	Principle 1 - Search references	237
	<i>Search references and purpose of a register</i>	238
	<i>Establishing purpose of a register</i>	239
7.5	Principle 2 - Use of information from register	241
	<i>Council of Europe Recommendation R(91)10</i>	242
	<i>Application to every person</i>	242

	<i>Layout</i>	242
7.6	Principle 3 - Electronic transmission of personal information from public register	243
	<i>Manual to computerised registers</i>	243
	<i>Privacy risks of electronic transmission</i>	243
7.7	Principle 4 - Charging for access to public register	246
	<i>Third party charging</i>	246
7.8	Proposed new principle - bulk disclosures	248
	<i>Obtaining bulk information from a register</i>	248
	<i>Publication of a register in its entirety</i>	250
7.9	SECTION 60 - Application of information privacy principles and public register privacy principles to public registers	251
	<i>Application and savings provisions - sections 7, 8 and 60</i>	251
	<i>“Reasonably practicable” in section 60(2)</i>	253
7.10	SECTION 61 - Complaints relating to compliance with principles	253
7.11	SECTION 62 - Enforceability of principles	254
7.12	SECTION 63 - Codes of practice in relation to public registers	254
7.13	SECTION 64 - Effect of code	256
7.14	SECTION 65 - Power to amend Second Schedule by Order in Council	257
	<i>Use of Orders in Council to bring statutory registers into scheme</i>	257
	<i>Domestic Violence Act regulations</i>	258
7.15	Statutory mechanisms for suppression of details on registers	259
	<i>Suppression mechanisms in existing statutes</i>	259
	<i>Harassment</i>	260
	<i>Discussion paper</i>	261
	<i>Proposed new public register privacy principle</i>	262
	<i>Mechanism for obtaining suppression directions</i>	264
7.16	Interaction with Official Information Act and Local Government Official Information and Meetings Act	265
 PART VIII: COMPLAINTS		
8.1	Introduction	267
	<i>New Zealand complaints model</i>	268
	<i>Role of the courts</i>	268
	<i>Complaints or reviews?</i>	269
8.2	SECTION 66 - Interference with privacy	270
	<i>Clarification of interaction between subsections (1) and (2)</i>	270
8.3	SECTION 67 - Complaints	271
8.4	SECTION 68 - Mode of complaint	272
8.5	SECTION 69 - Investigation of interference with privacy of individual	272
8.6	SECTION 70 - Action on receipt of complaint	273
	<i>Notification</i>	273
	<i>Deferral</i>	273
	<i>Preliminary inquiries</i>	273
	<i>Complaints beyond jurisdiction</i>	275
8.7	SECTION 71 - Commissioner may decide to take no action on complaint	275
	<i>Deferral of complaints</i>	276
	<i>Grounds for deferral</i>	277
	<i>Limitation period</i>	279
8.8	SECTION 72 - Referral of complaint to Ombudsman	279
8.9	SECTION 72A - Referral of complaint to Health and Disability Commissioner	279
8.10	SECTION 72B - Referral of complaint to Inspector-General of Security and Intelligence	280

8.11	SECTION 73 - Proceedings of Commissioner	280
8.12	SECTION 74 - Settlement of complaints	280
8.13	SECTION 75 - Parties to be informed of result of investigation	281
8.14	SECTION 76 - Compulsory conferences	282
8.15	SECTION 77 - Procedure after investigation	282
8.16	SECTION 78 - Procedure in relation to charging	282
8.17	SECTION 79 - Breaches of certain principles occurring before 1 July 1996	283
8.18	SECTION 80 - Commissioner to report breach of duty or misconduct	284
8.19	SECTION 81 - Special procedure relating to intelligence organisations	284
8.20	SECTION 82 - Proceedings before Complaints Review Tribunal	285
	<i>“Specialist” tribunal</i>	285
	<i>Section 82</i>	286
	<i>Enforcement of assurances</i>	287
8.21	SECTION 83 - Aggrieved individual may bring proceedings before Complaints Review Tribunal	288
8.22	SECTION 84 - Remedies that may be sought	289
8.23	SECTION 85 - Powers of Complaints Review Tribunal	289
8.24	SECTION 86 - Right of Proceedings Commissioner to appear in proceedings	289
8.25	SECTION 87 - Proof of exceptions	289
8.26	SECTION 88 - Damages	290
8.27	SECTION 89 - Certain provisions of Human Rights Act 1993 to apply	290
 PART IX: PROCEEDINGS OF COMMISSIONER		
9.1	Introduction	291
9.2	SECTION 90 - Procedure	292
9.3	SECTION 91 - Evidence	292
9.4	SECTION 92 - Compliance with requirements of Commissioner	293
	<i>Sanction for breach of time limits</i>	294
9.5	SECTION 93 - Extension of time limit	295
	<i>No provision for multiple extensions</i>	295
9.6	SECTION 94 - Protection and privileges of witnesses etc	295
	<i>1997 amendments - subsections (1A) and (1B)</i>	295
	SECTION 95 - Disclosures of information etc	297
	SECTION 96 - Proceedings privileged	298
 PART X: INFORMATION MATCHING		
10.1	Introduction	300
	<i>What is information matching?</i>	300
	<i>Pros and cons of data matching</i>	301
	<i>Controls on data matching</i>	303
	<i>Information matching not prohibited</i>	303
	<i>Legitimising data matching</i>	305
10.2	SECTION 97 - Interpretation	306
	<i>Further definitions</i>	306
	<i>Adverse action</i>	306
	<i>Authorised information matching information</i>	307
	<i>Authorised information matching programme</i>	307
	<i>Discrepancy</i>	308
	<i>Information matching programme</i>	308

	<i>Information matching provision</i>	309
	<i>Information matching rules</i>	310
	<i>Monetary payment</i>	310
	<i>Specified Agency</i>	310
10.3	SECTION 98 - Information matching guidelines	312
	<i>Paragraph (c)</i>	313
	<i>Paragraph (e)</i>	313
	<i>Paragraph (f)</i>	315
10.4	SECTION 99 - Information matching agreements	316
	<i>Upside</i>	316
	<i>Downside</i>	316
10.5	SECTION 100 - Use of results of information matching programme	317
10.6	SECTION 101 - Further provisions relating to results of information matching programme	318
	<i>Inland Revenue Department</i>	318
10.7	SECTION 102 - Extension of time limit	319
	<i>Which time limit?</i>	319
10.8	SECTION 103 - Notice of adverse action proposed	320
	<i>Subsection (1A) - the Customs Match</i>	320
10.9	SECTION 104 - Reporting requirements	323
	<i>Australian equivalents</i>	323
10.10	SECTION 105 - Information matching programmes to be reported on in annual report	324
	<i>Costs of monitoring and assessment</i>	325
10.11	SECTION 106 - Review of statutory authorities for information matching	327
10.12	SECTION 107 - Amendment of information matching rules	327
	<i>Rule 1 - Notice to individual affected</i>	328
	<i>Rule 2 - Use of unique identifiers</i>	329
	<i>Rule 3 - On-line transfers</i>	330
	<i>Rule 4 - Technical standards</i>	331
	<i>Rule 5 - Safeguards for individuals affected by results of programmes</i>	331
	<i>Rule 6 - Destruction of information</i>	332
	<i>Rule 7 - No new databank</i>	332
	<i>Rule 8 - Time limits</i>	333
	<i>Defining terms</i>	334
10.13	SECTION 108 - Avoidance of controls on information matching through use of exceptions	334
10.14	SECTION 109 - Avoidance of controls on information matching through use of official information statutes	335
PART XI: LAW ENFORCEMENT INFORMATION		
11.1	Introduction	337
	<i>Wanganui Computer Centre Act 1976</i>	338
	<i>On-line access</i>	340
11.2	SECTION 110 - Interpretation	342
	<i>Accessing and holder agencies</i>	342
	<i>Law enforcement information</i>	342
	<i>Local authority</i>	342
11.3	SECTION 111 - Access by accessing agencies to law enforcement information	343
11.4	SECTION 112 - Local authorities may be authorised to have access to law enforcement information	344
	<i>Current local authority access</i>	344
	<i>Need for local authority access</i>	345
	<i>Amendments if local authority access retained</i>	345
11.5	SECTION 113 - Amendment to Fifth Schedule	346

11.6	SECTION 114 - Expiry of power to amend Fifth Schedule by Order in Council	348
PART XII: MISCELLANEOUS PROVISIONS		
12.1	Introduction	349
12.2	SECTION 115 - Protection against certain actions	350
12.3	SECTION 116 - Commissioner and staff to maintain secrecy	351
12.4	SECTION 117 - Consultation with Ombudsmen	352
12.5	SECTION 117A - Consultation with Health and Disability Commissioner	353
12.6	SECTION 117B - Consultation with Inspector-General of Intelligence and Security	353
12.7	SECTION 118 - Corrupt use of official information	353
12.8	SECTION 119 - Exclusion of public interest immunity	354
12.9	SECTION 120 - Adverse comment	355
12.10	SECTION 121 - Delegation of functions or powers of Commissioner	356
12.11	SECTION 122 - Delegate to produce evidence of authority	356
12.12	SECTION 123 - Revocation of delegations	356
12.13	SECTION 124 - Delegation of powers by local authority	356
12.14	SECTION 125 - Delegation of powers by officers of local authority	357
12.15	SECTION 126 - Liability of employer and principals	358
12.16	SECTION 127 - Offences	358
	<i>Discussion paper and submissions</i>	358
	<i>Impersonating the individual concerned</i>	359
	<i>Destroying requested information to deny access</i>	360
	<i>Computer crimes</i>	360
	<i>Time for laying information</i>	361
12.17	SECTION 128 - Regulations	362
12.18	SECTION 129 - Amendments, repeals and revocations	362
	<i>Repeal of Wanganui Computer Centre Act</i>	363
	<i>Coerced access requests - medical records</i>	366
12.19	SECTION 130 - Final report of Wanganui Computer Centre Privacy Commissioner	367
12.20	SECTION 131 - Privacy Commissioner to complete work in progress of Wanganui Computer Centre Privacy Commissioner	367
12.21	SECTION 132 - Savings	368
12.22	SECTION 133 - Transitional provisions	368
SCHEDULES		
13.1	Introduction	369
13.2	First Schedule	369
13.3	Second Schedule	370
13.4	Third Schedule	370
13.5	Fourth Schedule	370
13.6	Fifth Schedule	370
13.7	Sixth Schedule	371
13.8	Seventh Schedule	371
13.9	Eighth Schedule	371
13.10	New Schedules	371
SUMMARY OF RECOMMENDATIONS		373

APPENDICES

A.	Acknowledgments	389
	<i>Staff of the Office of the Privacy Commissioner</i>	389
	<i>Preliminary input</i>	389
	<i>Discussion papers and consultation processes</i>	390
	<i>Specialist consultation</i>	391
	<i>Assistance from overseas</i>	391
	<i>Miscellaneous assistance</i>	392
B.	List of submissions	393
C.	Recent overseas privacy legislation	397
D.	Legislative background	399
	<i>Legislative influences</i>	399
	<i>List of Privacy Commissioners</i>	400
E.	PCO drafting style changes	401
F.	Reports to the Minister of Justice	403
G.	Commissioner's functions under other statutes	405
	<i>Complaints mechanisms</i>	405
	<i>Commissioner's approval</i>	405
	<i>Consultations</i>	406
	<i>Appointment to other bodies</i>	406
	<i>Codes of practice</i>	406
	<i>Information matching</i>	407
H.	Tables of equivalent provisions	409
	<i>Right of access and correction</i>	409
	<i>Savings</i>	409
	<i>Reasons for refusing access to information</i>	410
	<i>Procedural provisions relating to access to and correction of information</i>	410
	<i>Complaints and investigations</i>	411
	<i>Proceedings</i>	411
	<i>Miscellaneous provisions</i>	412
I.	List of public registers	413
J.	Complaints graphs	415
	<i>Incoming complaints</i>	415
	<i>Nature of complaints</i>	416
	<i>Resources deployed and complaints queue</i>	418
	<i>Closure and complaint outcomes</i>	420

LIST OF FIGURES

1	<i>Discussion papers and numbers of submissions</i>	3
2	<i>Geographical spread of 0800 calls received in June/July 1997</i>	112
3	<i>Privacy Issues Forum</i>	113
4	<i>Ombudsmen consultations</i>	352
J1	<i>Complaints received</i>	415
J2	<i>Complaints carried forward at year end</i>	416
J3	<i>Access complaints as a percentage of total annual complaints</i>	416
J4	<i>Ratio of access complaints to other complaints</i>	417
J5	<i>Public/private sector breakdown of complaints</i>	417
J6	<i>Disclosure complaints by sector</i>	418
J7	<i>Number of investigators</i>	418
J8	<i>Complaints on hand per investigator</i>	419
J9	<i>Complaints queue</i>	419
J10	<i>Complaints received/closed on annual basis</i>	420
J11	<i>Complaints received/closed on quarterly basis</i>	420
J12	<i>Analysis of complaints received to 30 June 1997</i>	421

Preface

P

The report has four parts:

- Introductory material;
- Part by Part analysis;
- Summary of recommendations;
- Appendices.

The *Introduction* sets the Privacy Act and this review into context. It discusses the international, technological and economic environment, legislative evolution, and the conduct of the review. It also introduces themes that are developed further in the report.

The *Part by Part analysis* covers the entire Act from section 1 to its Eighth Schedule. The material is presented in 12 chapters corresponding to the 12 Parts of the Act and a thirteenth devoted to the schedules. Each chapter begins with introductory material and then works systematically through the relevant sections and provides recommendations. As individual sections of the Act interact with each other, I have extensively cross referenced.

The *Summary of Recommendations* follows. The recommendations are derived from the analysis and collected in one series.

The *Appendices* elaborate upon and list some of the material referred to in the report. Lists are included of those who made submissions, overseas legislation, public registers and corresponding provisions in the official information statutes.

SOURCES OF INFORMATION

The Privacy Act consists of 133 sections, 8 schedules and 100 pages. I discuss each section of the Act regardless of whether amendment is desirable. Not surprisingly this has led to a relatively long report. To contain the length I have avoided reprinting extracts from the Act. To obtain a full appreciation of the issues and recommendations it is necessary to refer to a copy of the Privacy Act.

The submissions referred to in the report, and others not referred to, are available in four volumes from my office. I have highlighted quotations from submissions whether or not they support the recommendations that I make. Some have been condensed or edited. There is a variety of genuinely held views on many of the issues tackled in the report and the quotations are intended to illustrate that. I do not necessarily endorse the sentiments expressed.

The footnotes include references to my earlier reports to the Minister of Justice, reports by official bodies, overseas privacy laws, case notes, Tribunal decisions and text books. Two of the most frequently cited texts are:

- Dr Paul Roth, *Privacy Law and Practice*, Butterworths, 1995-1998, cited as *Privacy Law and Practice*; and
- Ian Eagles, Michael Taggart and Grant Liddell, *Freedom of Information in New Zealand*, Oxford University Press, 1992, cited as *Freedom of Information in New Zealand*. *Privacy Law and Practice* is a comprehensive loose-leaf work on the Act. It contains the complete text of the key international instruments referred to at various places in this report. *Freedom of Information in New Zealand* is the leading text on the official informa-

tion legislation although it does not take account of developments since December 1991 such as the enactment of the Privacy Act.

TERMINOLOGY

Any reference to “the Act” or a section is, unless the context suggests otherwise, a reference to the Privacy Act 1993 or a section in the Act. Similarly, “principle” is to be taken to be an “information privacy principle” or, if the context suggests, a “public register privacy principle”.

Other abbreviations include:

- “Convention No 108” - the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, 28 January 1981;
- “case note” - a case note released by the Office of the Privacy Commissioner;
- “discussion paper” - one of the 12 discussion papers released by the Office of the Privacy Commissioner, June to September 1997;
- “EU” - European Union;
- “EU Directive on Data Protection” - the EU Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data, 24 October 1995;
- “OECD” - the Organisation for Economic Cooperation and Development;
- “OECD Guidelines” - the OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, 23 September 1980;
- “Recommendation R(91)10” - Council of Europe Recommendations on Communication to Third Parties of Personal Data held by Public Bodies, 9 September 1991.
- “Tribunal” - the Complaints Review Tribunal.

The report was mostly finalised in July 1998 so does not generally include reference to developments between that date and the time of publication. For example, during that time advice was received concerning the enactment of the UK Data Protection Bill, referred to in the report, and moves towards bringing magazines within the Press Council scheme.

The tabs shown on the right hand side of the pages of the report give section references (upper tab) and page references (lower tab).

Overview

Introduction

Privacy has been a significant national and international concern for over 30 years. During the 1960s and 1970s a range of concerns about the relationship between citizen and state emerged with the perceived growing threat of large computer databanks. The 1980s saw significant efforts at international privacy standard setting and legislative efforts to provide adequate protection to privacy with 1984 a favourite time for reflection on technological challenges to individual privacy. The 1990s have seen technological advances undreamed of by George Orwell with the worldwide linking of computers, the electronic tracking of consumers and citizens and advances from the microscopic work of the Human Genome Project through to global satellite surveillance from outer space.

Together with the unease at entering a “brave new world” there remain a host of routine, but hugely important, privacy issues in everyday lives. Issues revolving around the information held on personnel files. The maintenance of blacklists in employment and housing. The accuracy of information upon which credit decisions are made. The wish to have our homes secure from unwanted intrusions.

It is into this environment that the Privacy Act 1993 was enacted. The Act covers a variety of matters as will be apparent from reading this report. Two central features are the establishment of a Privacy Commissioner and a set of information privacy principles. The Privacy Commissioner is an independent official. One function is to periodically review the operation of the Act. It is upon that task that I have been engaged in preparing this report. The information privacy principles apply to all agencies in the public and private sectors and govern the collection, holding, use and disclosure of personal information. Individuals have certain entitlements under the Act including to access and seek correction of personal information held by agencies and to obtain redress for interferences with their privacy.

The privacy regime established by the Privacy Act accords with obligations assumed by New Zealand as part of its membership of the United Nations and OECD. The Act follows well established models in Europe, North America and Australia, although it has a number of advanced features relating to its private sector coverage and its application to all personal information. It is noticeably less bureaucratic than early European models.

The Act has notably advanced the position of individuals in New Zealand in just a few short years. It is sometimes easy to forget quite how far we have come. For example, note:

- New Zealanders can access their own medical records. One might reflect upon the fact that individuals do not have this right in most parts of Australia and North America.
- New Zealanders are entitled to seek correction of information held on credit reporting agencies’ files if it is inaccurate. There was no right even to see the information prior to 1993.
- People may have access to information held on their personnel file. This has been an entitlement for employees in the public sector since the 1980s but it has only been

with the enactment of the Privacy Act that all employees enjoy this important right.

- Before the Privacy Act businesses and government agencies did not have to be open as to what they wanted personal details for and who they were going to share these with.
- Problems in other jurisdictions have not arisen here. For example, Australian lawyers report a lack of remedy for tenants wrongly placed on housing black lists.
- A simple complaints mechanism with an ombudsman-like investigation of privacy complaints with a non-adversarial approach.
- Outsourcing and privatisation do not deprive citizens of privacy rights in relation to personal data previously held by government agencies.

The report which follows examines provisions in the Act in detail and makes a number of recommendations. The purpose of the introductory and background material is to give an overview as to the context in which the Act operates and to introduce a number of the 154 recommendations.

REVIEW PROCESSES

Section 26(1) requires the Privacy Commissioner to review the operation of the Act as soon as practicable after the Act has been in force for three years and thereafter at intervals of not more than five years. The Commissioner's review concludes with a report to the Minister of Justice of the findings with recommendations as to any necessary or desirable amendments to the Act.

Section 26 does not require the review to be conducted in any particular way. However, I decided that it was desirable to consult with those affected - not just with government and business but with the public as well. I told the Minister of Justice of my intentions and a statement to this effect was made by the Minister in Parliament in August 1996.

Commencement of the review

Preparatory steps were taken during 1995 and the first half of 1996. Enquiries were made of overseas Commissioners as to recent reviews of their own legislation. A study was made of notable features of overseas laws and recent international instruments. In August 1996 I wrote to the chief executives of Government departments seeking ideas for the review and their initial impressions of the Act's operation. In January 1997 a similar letter went to 10 representative bodies in the private sector. In February a questionnaire concerning Part X of the Act was circulated to agencies participating in authorised information matching programmes.

The public phase of the review started at about the time of the Act's fourth anniversary with the submission of this report to the Minister of Justice soon after the fifth. While my review has been under way there have been a number of continuing developments needing study. These have included:

- European elaboration of the implications of the EU Directive on Data Protection;
- a number of Complaints Review Tribunal decisions following the end of the three year transition period;
- a procession of reviews and legislative proposals in Canada and Australia.

Discussion papers

Many people with useful experience with the Act might have been discouraged by a single large consultation document. So my office released 12 short discussion papers over a period of several months allowing people to choose to contribute depending upon where their experience or interest lay. The first eight papers corresponded to relevant Parts of the Act while the balance took the themes of compliance and administration costs, interaction with other laws, intelligence organisations, and new privacy protections. They primarily drew upon ideas and issues generated or identified within my office or in responses to the earlier letters to departments, representative bodies and the information matching questionnaire.

FIGURE 1. DISCUSSION PAPERS AND NUMBERS OF SUBMISSIONS

No	Title	Month released 1997	Submissions received
DP1	Structure and scope	July	47
DP2	Information privacy principles	August	47
DP3	Access and correction	August	50
DP4	Codes of practise and exemptions	August	21
DP5	Public register privacy issues	September	31
DP6	Complaints and investigation	September	29
DP7	Information matching	September	13
DP8	Law enforcement information	July	31
DP9	Compliance and administration costs	September	27
DP10	Interaction with other laws	August	34
DP11	Intelligence organisations	August	25
DP12	New privacy protections	September	27

A good response was received to the discussion papers and the list of those who made submissions is set out in Appendix B. Submissions continued to be received beyond the closing date of 10 November 1997 but most were to hand by February 1998. The submissions were acknowledged, numbered and compiled into four volumes. These were provided to the Ministry of Justice in February 1998 and were then made available for inspection or purchase from my office.

In November 1997 I held a series of consultation meetings in the four main centres. These enabled people who had made written submissions to elaborate upon issues of concern. A further series of meetings between myself, my staff, and certain invited experts, were held during December. Details are given in Appendix A. A consultation meeting was held with local authorities.

Completion of the report

During 1998 I continued to study the submissions and research the issues raised. In some cases further details were solicited from the person making the submission. In other cases, specialist drafting or technical advice was taken.

As material was prepared I took the opportunity to further consult people with relevant expertise and some agencies which might be specifically affected by recommendations under consideration. Most of the report was written by the end of July 1998.

THEMES IN THE REPORT

Although I consider the Privacy Act is firmly “on the right track”, I make 154 recommendations. It should not be inferred from the number of recommendations that the Act needs any major change of direction. There are proposals to rewrite provisions to make the Act more effective or understandable. Some new rights should be conferred or existing rights extended. I have proposed restrictions in the Act where I believe this will result in compliance cost reductions without significantly diminishing privacy rights. However, many of the recommendations can be characterised as being of a technical or “fine tuning” kind. Nonetheless, some of the 154 recommendations do raise matters of importance.

The recommendations in the report may be categorised in a variety of ways. A simple categorisation is used in the report itself, which examines the Act Part by Part, by linking the recommendations to the sections to which they relate. Accordingly, a reader interested in the relevant recommendations concerning access to personal information will find them in the part of the report relating to section 6 (information privacy principle 6) and sections 27 to 45. Those interested in recommendations concerning privacy officers will look at the material concerning section 23.

There are a number of themes in the recommendations:

- coverage of the Act;
- enhancement of individual rights;
- effectiveness of my Office;
- interaction with other laws;
- compliance and administration costs;
- ease of use of the Act;
- “adequate protection” in terms of the EU Directive.

The recommendations referred to in the following material are not exhaustive and many have been abbreviated and paraphrased.

Coverage of the Act

A principal feature of the Act is its broad coverage:

- it covers all “agencies” whether in the public or private sectors; and
- it applies to all “personal information”.

Broad coverage gives confidence that the information privacy principles apply in nearly all circumstances. The greater the inroads into the types of agencies or information covered, the greater the possibility of privacy being left unprotected. The broad coverage of the Act is also the surest guarantee that our law will be considered to offer “adequate protection” in respect of the tests established in the EU Directive on Data Protection. It also avoids compliance costs, creates certainty, avoids demarcation disputes or gaps between codes of practice.

Coverage is not absolute. There are bodies which are expressly excluded from the definition of “agency”. There are also partial exemptions applying to particular classes of agency or information. I examined the existing coverage of the Act to see whether changes should be made to extend or restrict the coverage.

Some recommendations are:

- the exemptions applying to the House of Representatives and MPs should be considered by a committee of Parliament - recommendations 5 and 6;
- consideration should be given to replacing the Parliamentary Service Commission’s total exemption with a partial exemption - recommendation 7;
- the partial exemption for the Parliamentary Service should be repealed or further restricted - recommendation 8;
- the exemption for the Ombudsmen should be repealed - recommendation 10;
- consideration should be given to narrowing the Royal Commission exemption - recommendation 81;
- the domestic affairs exemption should be restricted where an individual falsely represents the position to an agency - recommendation 82;
- the partial exemption for intelligence organisations should be further narrowed - recommendation 83;
- the IRD’s exemptions in section 101(5) and information matching rule 6(3) should be limited - recommendation 126.

There has been considerable interest in the exemption which applies to the news media in their news activities. I propose no change. The exemption is discussed at various places in the report in particular at paragraphs 1.4.49 to 1.4.62 and at paragraphs 4.4.49 to 4.4.55.

Enhancement of individual rights

The objective of the privacy law is to “promote and protect individual privacy”. I have examined the Act to consider whether it is effective in that respect and make a number of recommendations to better promote and protect privacy by enhancing individual rights and entitlements.

The 12 information privacy principles, and other controls relating to public registers and information matching, are at the heart of the Act. Aspects of the regime can be modified in certain ways by codes of practice. Through a mixture of constraints on agencies and entitlements for individuals these provisions establish a framework to protect individual privacy rights.

In the review I have studied ways in which privacy rights for individuals can be enhanced consistently with the international approach to the protection of privacy while taking account of competing interests. Few of the enhancements that I propose are entirely novel. Most involve adjustments to existing entitlements or the borrowing of ideas from international or overseas initiatives. In a number of cases I suggest specific entitlements consistent with the existing general entitlements. For example, I make proposals to change the information privacy principles and public register privacy principles to address direct marketing issues. Although the specific provisions will be new they will give effect to an objective of the existing principles - constraining a secondary use of information without the knowledge or authorisation of the individual.

Some recommendations are:

- allowing codes of practice to confer certain further entitlements - recommendations 18, 27, 35(b);
- requiring compliance with principle 3 where personal information is being collected directly from an individual for research or statistical purposes - recommendation 21;
- amending principle 7 so that agencies are obliged to inform requesters of their correction statement entitlements - recommendation 24;
- conferring an entitlement to require personal information to be deleted from direct marketing lists - recommendation 25;
- establishing entitlements to access information held by a private sector agency as a legal right in cases of private prosecutions - recommendation 36;
- requiring a requester to be given, without having to ask, the grounds in support of the reasons for withholding evaluative material - recommendation 54;
- requiring agencies to make reasonable endeavours to process urgent requests with priority - recommendation 67;
- allowing individuals to ask that their access requests not be transferred - recommendation 68;
- conferring further entitlements in respect of personal information held by intelligence organisations - recommendation 83;
- constraining bulk release of personal information from public registers for direct marketing - recommendation 91;
- creating enforceable remedies in relation to breach of public register privacy principles - recommendation 95;
- providing for suppression of information on public registers for reasons of personal safety or harassment - recommendations 97, 98, 99;
- enabling certain jurisdictional matters to be taken by a complainant to the Complaints Review Tribunal - recommendation 105;
- criminalising the knowing destruction of documents in order to evade an actual access request - recommendation 149;
- outlawing coerced access requests - recommendations 151, 152.

I do not consider that these changes will entail any significant compliance costs.

Effectiveness of Office of the Privacy Commissioner

The Privacy Commissioner established by the Act is given a number of tasks. The Act grants various powers to enable those tasks to be effectively performed. I have considered whether the provisions of the Act are adequate, or can be improved, to ensure that my Office is able to perform effectively. For the most part I believe that the provisions in the Act are satisfactory. Nonetheless, I have identified a number of areas where potential effectiveness will be enhanced by amendment to the Act.

Relevant recommendations include:

- enhancing powers to address privacy issues by codes of practice - recommendations 18, 74;
- excluding the official information statutes from determining questions of release of information from public registers - recommendation 100;
- clarifying requirements concerning action on receipt of complaints - recommendation 104;
- establishing a process for referring jurisdictional questions to the Complaints Review Tribunal - recommendation 105;
- establishing a formal power to defer complaints - recommendation 106;
- seeking adequate funding so that complaints may be processed with due expedition - recommendation 108;
- enabling the enforcement of assurances - recommendation 112;
- enabling requirements to be complied with within an abbreviated time period - recommendation 114;
- varying the information matching guidelines to require examination of a proposed programme's compliance with Part X - recommendation 124;
- requiring periodic review of information matching agreements - recommendation 125;
- funding information matching monitoring activities by the agencies undertaking matching - recommendation 132;
- extending the limitation period for offences under the Act - recommendation 150.

Interaction with other laws

The Privacy Act is obviously not the only law bearing upon the handling of personal information. These include, amongst others, laws concerning:

- obtaining information - such as the statutory powers of the DSW to obtain information and documents from individuals and businesses;
- holding or retaining information - such as the Archives Act and requirements in tax laws requiring the retention of financial records;
- disclosing information - such as the secrecy provisions applied to certain government agencies prohibiting the disclosure of information;
- accessing information - such as the public register provisions and the Official Information Act.

The Act currently spells out how it is to relate to other pieces of legislation. Generally it provides that the information privacy principles are subordinate to provisions in most other enactments.

I have considered whether the way the Act currently deals with the interaction of other laws is satisfactory. One of the main problems that I have attempted to address concerns the lack of awareness by some users of the Act of the provision saving the effect of other laws. Amongst other things, my recommendations seek to make the interrelationship plainer so as to reduce misunderstanding. The term “savings” is a technical legal term which is not readily understood by lay readers of the Act. Some would appear to be unaware that the privacy principles do not override other laws.

Relevant recommendations include:

- changing the marginal notes to the savings provision in section 7 to direct users of the Act more clearly to its relevance - recommendation 2;
- moving material relating to the saving of the effect of other laws into the various principles as new exceptions - recommendations 30, 31(a), 33;
- relocating the provisions saving the withholding effect of other laws into Part IV as a reason to withhold information - recommendation 32;
- refashioning the savings provision concerning enactments imposing more restrictive obligations of non-disclosure - recommendation 33;
- providing for the expiry of the saving of regulations allowing for refusal of access requests - recommendation 34;
- clarifying the relationship between the principles and public register provisions - rec-

- recommendations 92-95;
- bringing provisions in other statutes into the public register regimes of the Privacy Act and Domestic Violence Act - recommendations 96 and 97;
- excluding the official information statutes from questions of release of information from public registers - recommendation 100;
- tidying up the provisions concerning the transfer of complaints between, and consultation with, the Privacy Commissioner and other statutory complaints bodies - recommendations 102, 107, 145 and 146.

Compliance and administration costs

Business compliance cost reduction has been an issue for government in recent years. Indeed, the matter has been a central feature leading to the present design of the Act. Most notable is the absence of a registration or licensing system which is the norm in Europe. The Privacy Act adopts an outcomes-oriented approach whereby the Act prescribes the standards but agencies have a great deal of flexibility in the way that they may comply with them. In my review I examined various features which contribute to the low compliance costs imposed by the Act and examined whether it would be possible through amendment to the Act to improve the position even further with respect to compliance costs.

Compliance costs revolve around the costs borne by agencies in complying with the requirements of the Act. It should not be assumed that, in the absence of an Act, there would be an absence of costs associated with meeting privacy risks and issues. Where statutes do not broadly cover privacy issues a variety of sectoral laws is normally combined with voluntary self regulation and laws relating to confidentiality. All these involve compliance costs. Costs borne by agencies cannot be considered in isolation from the costs imposed upon individuals in exercising their rights and entitlements under the Act. Accordingly, I also examined the regime established by the Act in that regard particularly with respect to charges that individuals may have to pay in order to have access to information or to seek to have it corrected.

Frequently issues of compliance costs interrelate with the administration costs of agencies established by a law. I am of the opinion that the work that my office does or might undertake in relation to education and publicity, particularly in offering compliance advice, contributes to minimisation of compliance costs among agencies. There are severe restrictions upon what I can attempt on my present budget given the need to apply resources to a significant complaints backlog. A 12 month queue before complaints are investigated is not only unfair to the complainants, and may undermine the credibility of the processes established, but also increases costs of the respondent agencies. In particular, where there is a continuing relationship between an individual and an agency, whether as customer, employee or otherwise, there is a great deal to be said for being able to promptly tackle the complaint through the Act's conciliatory processes which frequently lead to settlements which may often enable the relationship to continue. A delay in commencing the investigation also means that the events are not so fresh in people's minds leading to inefficiencies and problems in the investigation process and potential problems for the agency establishing its position, and may permanently sour the relationship.

In respect of the problem of administration costs, I believe that the solution is primarily to be found in the application of appropriate funding to meet the level of complaints being processed. Nonetheless, I have examined the provisions of the Act to see whether any amendments are desirable to ameliorate the problems. The recommendations I have made will contribute to the current low costs of compliance and help to prevent rises in costs in the future. I have considered requiring applicants to meet some costs of processing certain applications and giving me more statutory discretion to defer investigating complaints where it is reasonable that the individual first pursues an alternative.

A number of recommendations would improve ease of use of the Act. They also have an objective of reducing compliance costs.



Recommendations include:

- limiting information privacy principle 12(2) solely to the reassignment of unique identifiers originally generated, created or assigned by a public sector agency - recommendation 28;
- adopting a transborder data flow provision designed to have the least compliance cost effect on business - recommendation 35(a);
- repealing provisions for the preparation of a nationwide directory of personal information or, if provision for a directory is retained, requiring the Commissioner to have regard to compliance costs when determining whether or not to prepare a directory - recommendations 40, 42;
- permitting agencies to choose a privacy officer who is not within that agency - recommendation 44;
- entitling public sector agencies to make a reasonable charge for making information available to a foreigner who makes the request from overseas - recommendation 62;
- allowing exemptions to be obtained from having to deal with an individual's access request for a period where it can be shown that the individual has lodged requests of a repetitious or systematic nature which would unreasonably interfere with the operation of the agency and amount to an abuse of the right of access - recommendation 66;
- allowing exemptions to be obtained in relation to principle 9 (retention of information) - recommendation 79;
- enabling liability to be shared between an agency and individual where that individual, in a domestic or household capacity, misleads the agency into wrongly disclosing information - recommendation 82;
- enabling all charging complaints to be dealt with by the Privacy Commissioner without the prospect of further Tribunal proceedings - recommendation 110;
- integrating local government delegation provisions into a more convenient statutory location - recommendation 147.

Recommendations relevant to the administration costs of my office include:

- providing for the Commissioner to put a funding case directly to Treasury and relevant Ministers - recommendation 37;
- repealing provision for the Commissioner to publish a directory of personal information or alternatively transferring the function to the Ministry of Justice - recommendations 40 and 41;
- empowering the Commissioner to require a representative body to undertake public notification of an application for a code - recommendation 77;
- empowering the Commissioner to require an applicant for a section 54 exemption to publicly notify the application - recommendation 80;
- enabling the Commissioner formally to defer certain types of complaints - recommendation 106;
- funding the office so that complaints can be processed with due expedition - recommendation 108.

Ease of use of the Act

In many cases, I am satisfied that the substantive law bearing on an issue is appropriate and yet some people have found provisions difficult to follow. My suggestions will help to achieve the law's objectives through better agency compliance and better understanding of the rights of individuals.

My recommendations try to avoid substantial rewriting. This is to retain the benefits of familiarity gained by those using the Act over the last few years. So I have taken a minimalist approach which may deceive the reader into thinking that the changes are inconsequential. I am confident they have the potential to improve the Act's "user-friendliness" and thus avoid the chance of misinterpretation.

Some recommendations are:

- implementing changes in legislative drafting styles adopted by the Parliamentary Counsel Office and arranging a full reprint - recommendations 1, 4;

- making marginal notes and headings more informative - recommendations 2, 133;
- providing more useful comparative notes to equivalent provisions in the official information legislation - recommendation 3;
- altering definitions - recommendations 13, 14, 15, 50, 117-121, 137;
- replacing complex provisions with clearer provisions - recommendations 17, 64, 154;
- using the phrase “purpose or purposes” in the principles - recommendation 19;
- simplifying the provisions relating to the impact of other laws and relocating them to where users would expect to find the content - recommendations 30-33;
- simplifying the layout, and clarifying the content, of the withholding grounds - recommendations 47, 48, 52, 57, 58;
- amalgamating sections and relocating some material into schedules - recommendations 107, 145, 147;
- rewriting aspects of the information matching controls - recommendations 130, 135, 136, 137;
- removing spent or unnecessary provisions - recommendations 70, 102, 153.

“Adequate protection” in terms of the EU Directive

The EU Directive on Data Protection is required to be implemented in EU countries by October this year. The EU Directive will oblige member states to restrict the transfer of personal data to third countries if that data will not be subject to “adequate protection”. The existence of the Privacy Act is the best guarantee that the Europeans will accept that data on Europeans will be protected when transmitted to New Zealand. Generally speaking, New Zealand’s Privacy Act is perceived by most commentators as one of the best in the world outside Europe. Indeed, the protection that it offers to personal information is superior to that offered in many European jurisdictions, particularly in respect of information which is not “automatically processed”.

Nonetheless, I have carefully scrutinised the Act to be sure that its provisions will be judged by European standards to be “adequate”. To be adequate our law does not need to have identical provisions to the EU Directive. It is believed that the law will largely be judged in its totality. Our Act should, in general terms, pass such an adequacy test with flying colours.

However, there are two aspects which somewhat cloud this rosy picture. New Zealand’s law is in danger of failing an adequacy test in so far as it denies access rights to foreigners except when they are actually in New Zealand. This would effectively deny most Europeans one of the key data protection entitlements in any law. In my view, that should be put right as soon as possible.

The Office of the Privacy Commissioner, with its complaints jurisdiction, provides the independent national institution that is a central feature of an adequate system for the protection of privacy in European eyes. I have no doubt that the basic legislative arrangements for the Privacy Commissioner would be a feature which supports an adequacy case in European eyes. However, the underfunding of my office, which has led to complaints waiting in a 12-month queue, may cause EU Commissioners to question the adequacy of a central feature of our Act. An investigation delayed for that long can lose credibility as a compliance mechanism. It is important in this context, in my view, that this central aspect be put right.

Another issue relates to the possibility of European agencies diverting data transmissions through New Zealand to another country so as to circumvent the EU prohibition. This also should be put right.

Amongst my recommendations is one concerning the deletion of details from mailing lists which is modelled upon provisions in the EU Directive. Its current absence in our law is not likely to call into question the adequacy of New Zealand’s laws. Rather, the EU Directive provides a very promising model to copy from in according appropriate protection to the privacy of New Zealanders’ personal information.



Reference may be made to the recommendations:

- providing for the deletion or blocking of personal information held by an agency for direct marketing purposes - recommendation 25;
- providing a mechanism to enable mutual assistance to be extended to prohibit transborder data flows in circumstances where New Zealand is being used as a conduit for transfers designed to circumvent controls in EU and other privacy laws - recommendation 35(a);
- abolishing the standing requirements for foreigners to exercise access rights - recommendation 61;
- seeking that adequate funding should be made available so that the volume of complaints can be processed with due expedition - recommendation 108.

PRIVACY AT THE END OF THE TWENTIETH CENTURY

As we approach the dawn of the new millennium the Privacy Act provides a sound framework for addressing a range of privacy issues. Nonetheless, the appropriate protection of privacy necessarily is an ongoing process of refinement, evaluation, experimentation and consolidation. Technology will not remain static to suit a legal rule. Nor do the demands or expectations of the international community or New Zealanders. Already, I have identified issues which deserve further study and which may, at a future point, warrant amendment to the law.

The information privacy principles are based upon the 1980 OECD Guidelines. These represent a culmination of 1970s thinking on information privacy issues. Many experts believe that the OECD Guidelines have stood the test of time well and continue to be adequate to the task. However, from the early 1990s the OECD Guidelines have been subject to criticism from several quarters.¹ It has been suggested that they are not as technologically-neutral as first supposed with some key concepts, such as “data controller”, based upon understandings of existing information storage media, such as main-frame computers, rather than distributed computer networks or the Internet.

The OECD has seen scope for new principles. Its Guidelines on the Security of Information Systems (1992) and Guidelines on Encryption Policy (1997) each contained further principles relevant to information privacy. Guidelines are in preparation in relation to consumer protection in electronic commerce.

Other international bodies, such as the EU, Council of Europe and the ILO, to name but three, have also been involved in more specific standard setting in relation to information privacy issues. There has been concern to ensure that principles are up to the challenge of the “Information Society”.

In my review I have examined the laws of other countries and developing general international guidelines relevant to the better protection of individual privacy. As a result I have sometimes recommended the adoption of new provisions in our Act. A principal example is recommendation 25 in which I propose that individuals be entitled, as in the EU Directive on Data Protection, to have their names removed from direct marketing lists.

One of the discussion papers canvassed the possibility of new privacy protections and mentioned a number of the new principles being developed elsewhere. Twenty-seven submissions were received. In this report I have stopped short of recommending the adoption of the innovative principles mentioned in that paper. This is not because I believe that they are misconceived or of little importance. A number of new principles that have been proposed, such as those guaranteeing anonymity, promise to protect privacy better in some situations than our existing principles.

Some of the more novel ideas require more study than has been possible, or appropriate, in this review. Others may be more amenable to study when they have been fully imple-

¹ See, for example, John Gaudin, “The OECD Privacy Principles - Can They Survive Technological Change?” (1997) 3 *Privacy & Policy Reporter* 143 and 196.

mented in their own jurisdictions. For example, the Australian National Principles for the Fair Handling of Personal Information (February 1998) have been released on the understanding that they will be reviewed in 6 to 12 months time.

It is an active time for the development of privacy protections internationally. Amongst other developments to follow in the next couple of years are the:

- completion of national implementation of the EU Directive in Europe;
- initiatives in the USA involving enhanced self regulation and sectoral legislation;
- extension of privacy protection to the private sector in Canada;
- review of the wave of new privacy laws enacted between 1992 and 1997;
- conclusion of the international debate about access to encryption technology;
- implementation in Australia of the recent National Privacy Principles;
- International Standards Organisation's work directed towards establishing processes for certifying business compliance with privacy standards;
- development of privacy enhancing technologies enabling anonymous consumer transactions.

This is only a small list of what is happening internationally in respect of new privacy protections. There are a wide variety of ideas which have been advanced for taking the protection of privacy beyond the well trodden route of data protection principles found in the OECD Guidelines. A promising local example is the National Principles for the Fair Handling of Personal Information which has derived principles from the groundbreaking Australian Privacy Charter (1994). For example one principle, directed to a matter not currently addressed, is:

If we can (and you want to) we will deal with you anonymously

Wherever it is lawful and practicable, individuals should have the option of not identifying themselves when entering transactions.

Another novel principle, found in the Australian Privacy Charter, states:

“No disadvantage

People should not have to pay in order to exercise their rights of privacy described in this Charter (subject to any justifiable exceptions) nor be denied goods or services or offered to them on a less preferential basis. The provision of reasonable facilities for the exercise of privacy rights should be a normal operating cost.”

Another principle without precedent is under consideration in the context of the Human Genome Project and other initiatives involving genetic technology. People studying the issues are beginning to speculate whether notions of privacy, dignity and personal autonomy need to be strengthened by a “right *not* to know personal information” in certain circumstances. For instance, if one family member seeks a genetic test which reveals the probability of a debilitating condition should other family members be informed? Many individuals prefer to live their lives without any inkling of the probabilities of what the future holds for them. As genetic technology is further developed society may need to develop principles concerning the handling of such personal information which go beyond those in the OECD Guidelines of 1980.

Clearly there is much work to be done and challenges faced in the coming years. My confidence that the Privacy Act is soundly based, and works well in operation, should not be mistaken for complacency about the challenges to the protection of privacy. There are many chapters yet to be written in the report on our society's response to privacy issues but these will need to await further specialist examinations and the next periodic review of the Privacy Act.



Overview

Background

Privacy laws have not just sprung up out of nowhere. Privacy has developed from a number of imperatives.

INTERNATIONAL CONTEXT

There has been a worldwide resurgence of interest in information privacy law since the early 1990s. This is the third period of active international consideration of privacy issues following:

- initial articulation of the right to privacy in the late 1940s;
- detailed standard setting from the late 1970s to the early 1980s.

Most of the present activity arises for reasons of harmonisation within an enlarged European Union, the adoption of human rights in Eastern Europe and fresh examination of the issue by jurisdictions outside Europe.

Human rights origins

On 10 December 1948 the General Assembly of the United Nations proclaimed the Universal Declaration of Human Rights. This year marks the 50th Anniversary of that historic act. Article 12 of the Universal Declaration provided that:

“No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.”

Little attention was paid to states’ observance of the obligation to protect individuals against arbitrary interference with their privacy for the first 20 years of the Universal Declaration. However, in 1966 the right to privacy was incorporated into Article 17 of the International Covenant on Civil and Political Rights. The Covenant introduced two compliance mechanisms. The first is the requirement on states parties periodically to report to the UN Human Rights Committee in relation to compliance with the Covenant. New Zealand has cited the Privacy Act to the Committee in its report on compliance with Article 17.¹ The second is the entitlement of people in states, such as New Zealand, which have ratified the Optional Protocol to take complaints to the Human Rights Committee if their governments have failed to observe the Covenant and no local redress is available. Increasingly, privacy issues have been considered by the Human Rights Committee.

¹ See Ministry of Foreign Affairs and Trade, *Human Rights in New Zealand: Report to the United Nations Human Rights Committee under the International Covenant on Civil and Political Rights*, Information Bulletin No 54, June 1995, paragraphs 84-92.

The human rights approach to privacy issues has also been actively pursued in Europe. The Council of Europe was set up in 1949 with the atrocities experienced across the European continent fresh in states' minds. The Council sought to achieve a greater unity between its members to safeguard individual rights and realise the ideals and principles represented in the common European heritage. The Council's concern with privacy issues dates back to the European Convention for the Protection of Human Rights and Fundamental Freedoms of 4 November 1950. Article 8(1) of the Convention provided:

“Everyone has the right to respect for his private and family life, his home and his correspondence.”

A number of actions have been taken against European states for breach of that article.

Articulating privacy principles

General articulation of the right to privacy contained in the human rights instruments could not, of themselves, ensure the protection of privacy given their lack of detail and the challenges to privacy, especially the increasing technological challenges posed by large computer databases.

In 1968 the Council of Europe embarked upon an examination of whether member states' national laws were sufficient to protect personal privacy in the face of modern technology. This led, in the late 1970s, to the drafting by a committee of experts of what was to become the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (“Convention No 108”).

Convention No 108 has been hugely influential within Europe. Most member states enacted data protection laws along the lines of the Convention by the mid 1980s. There has been a further wave of data protection laws in the 1990s with the demise of communist regimes in Central and Eastern Europe. The governments and peoples of those countries wanted to embrace human rights standards. The Council of Europe is their prime reference point for privacy and other human rights.

Many of the data protection laws adopted as a result of Convention No 108 are being replaced this year by new laws brought about by the EU Directive on Data Protection. One of the most significant changes is the application of data protection laws to “manual data”. This highlights what has generally been seen as the most significant failing of Convention No 108. By concentrating solely on automatically processed data it failed to address the totality of information privacy.

In the late 1970s the OECD appointed a group of experts on transborder data barriers and privacy protection which was instructed to develop what were to become the OECD Guidelines. This group collaborated with the Council of Europe's experts which helped ensure consistency between the Guidelines and Convention No 108. The OECD Guidelines do not limit their application to automatically processed data and this may ultimately mean that they will be more enduring than Convention No 108. Most OECD states have adopted privacy legislation based upon the OECD Guidelines.

Although the Council of Europe and the OECD together include most of the developed world, their membership does not comprise the majority of the world's nations. The United Nations adopted Guidelines for the Regulation of Computerised Personal Data Files in 1990. These provide governments with a basis upon which they may legislate on privacy consistently with the approach taken in Europe and the OECD. However, the UN has not been active in the area of information privacy and its 1990 Guidelines are not seen as particularly influential. The UN guidelines, in a similar fashion to Convention No 108 a decade earlier, focus upon “computerised” data. In my view, it is no longer sensible to concentrate solely upon computerised data and an approach that covers all personal information, or at least principal categories of “manual data”, is far more appropriate.

European Union Directive on Data Protection

The European Union (formerly known as the EC and EEC) only became fully involved with data protection with the issue in 1995 of the Directive on Data Protection which seeks to harmonise the law across a Europe without frontiers. A draft of the Directive was issued by the EC Commission in 1990 with a European Parliament version released in 1992. The release of the draft Directive created a great deal of interest within and beyond the borders of the EU. The main international interest related to transborder data flows and the controls and prohibitions that EU States will be obliged to place on the export of personal data to jurisdictions which do not provide “adequate protection” for the data.

Work had already begun in New Zealand on developing information privacy legislation but undoubtedly the 1990 release of the draft directive spurred action which might otherwise have been delayed. New Zealand was hardly alone in responding to the EU Directive in that manner. Appendix C lists 22 other jurisdictions which have enacted general privacy or data protection laws since 1992. Experience in other similar countries sharing our values and commitment to human rights suggests that New Zealand would eventually have legislated in any case. However, the EU Directive hastened the legislation and meant that it was in the country’s economic interests to be able to show that our law applies “adequate protection” to data received from Europe.

Relevance of international considerations to the review

Parliament directed me in section 14(b) and 14(c) to take account of New Zealand’s international obligations, and to consider any developing international guidelines on privacy, when carrying out my functions. International considerations have borne upon my review in a number of ways. For example:

- New Zealand has accepted the OECD Guidelines and it has been necessary to ensure that any proposals for change are consistent with those Guidelines;
- the EU transborder data flow controls which guide European countries raise the prospect of barriers to the transmission of information and it has been desirable to identify and address any shortcomings to “adequate protection” in New Zealand law.

Throughout the report mention is made of the international dimension of the issues under review.

TECHNOLOGICAL CONTEXT

This year marks the 50th anniversary of the birth of the first modern computer. In 1948 a team from Manchester University built the world’s first computer with Random Access Memory which it dubbed “baby”. As with the other 1948 event, the Universal Declaration of Human Rights, the development was an outgrowth of Second World War experiences. The war effort had driven significant advances in technology and the pace has since accelerated. Fifty years on the world grapples with the “Y2K” or “millennium bug” problem which threatens to destroy or corrupt certain personal or other data and perhaps ruin businesses and harm individuals in the process. Undoubtedly, the baby has matured. In a single generation the ubiquitous computer has become pivotal to our lives, businesses and economies.

National and international responses to technology

By the late 1960s unease had emerged as to the effect that machines and technologies were having, or might have, on individual autonomy and privacy. The particular technological application at the forefront of public concern varies over time but the power of the computer is always central to the concerns. Capacity of computers was understood to be growing exponentially. In the late 1960s and the early 1970s, the focus tended to be upon the large central databases controlled by governments. Orwellian images of an all knowing Big Brother state were frequently mentioned. The fear of data surveillance also tended to merge into civil liberties concerns at law enforcement and state control.

Concern about the technological challenge to privacy posed by large databases was most vividly illustrated in New Zealand by the strong legal controls placed upon the law enforcement database in the Wanganui Computer Centre Act 1976. “Bugging” and “tap-



ping” were also high on the list of technologies raising privacy concerns. In the same period, a series of laws were enacted governing the interception of private communications.

The outcome of the technological concerns in the 1960s and 1970s, and the various legislative responses in developed countries, led to international moves to establish consistent sets of privacy principles. There was a concern that the technological challenges were such that a legislative response in any single country would be ineffective on its own. The Council of Europe Convention No 108 explicitly addressed “automatically processed data”. The OECD, in facing the same challenges at the same time, deliberately developed a set of technology neutral guidelines. The Privacy Act has followed this OECD approach.

The period since the OECD Guidelines and Convention No 108 has seen the common sets of principles applied to a succession of challenges posed by new technologies. There has been debate in the 1990s as to how successful the OECD Guidelines are and whether they are as truly technology neutral as first believed. For example, it is sometimes suggested that the notion of a “data controller” in the OECD Guidelines fits comfortably with 1970s understanding of mainframe computers but is less appropriately applied to distributed systems.

Some local technological issues

The period since 1993 has seen the introduction, or proposed introduction, of a number of technologies posing challenges for privacy of New Zealanders. For example we have seen the:

- nationwide introduction of caller ID;
- appearance of smartcards;
- commencement of government data matching;
- broad adoption of email for communications;
- rising popularity of the Internet;
- establishment of national sports drug testing;
- unveiling of plans to issue digitised photo ID driver licences;
- prospect of electronic road tolling and the tracking of motor vehicles;
- introduction of various swipe-card retail loyalty schemes;
- construction of CCTV surveillance systems in public places;
- electronic counting of votes;
- computerisation of public registers;
- almost universal adoption of Eftpos in retail outlets.

Some of these proposals have developed with a degree of study and consultation. However, in our rapidly changing technological world this is the exception rather than the rule. New technologies emerge, and existing technologies converge, at a fast pace and the market tends to dictate their adoption. New technologies are rapidly used by businesses and governments if they appear to offer efficiencies. Frequently, privacy is the loser, sometimes in small ways, sometimes in a quantum leap.

It is clear that there will be a host of new technological issues and challenges for privacy in the next five years. Undoubtedly the Internet will be a matter of interest as digital cash comes into use and the debate about access to encryption technology continues. I expect vehicle tracking and electronic road tolls to be a particular matter for study in New Zealand. We will in all likelihood see further convergence of technologies as particular applications are linked to computers directly or via the telecommunications network. We may see extended uses of older privacy-intrusive technologies such as those involving the interception of private communications, CCTV surveillance and drug testing. “Cutting edge” technologies like smart cards and biometric identification may be brought into wider use.

Benefits to privacy of technology

New technology is not always detrimental to privacy. I hope that ways may be found to

use technological advances for the benefit of individual autonomy instead of always seeing privacy as the loser or accepting some compromise which salvages some vestige of previously enjoyed privacy rights.

There is scope for the adoption of new Privacy Enhancing Technologies (PETs) so as to give individuals the opportunity to participate in anonymous transactions. The creation of transactional data trails in electronic commerce, using individuals' identities, poses a real risk of mass profiling and "dataveillance" to the detriment of individual privacy. I hope that privacy impact assessments of significant new proposals will increasingly identify opportunities for adopting PETs. I have already taken the view that an anonymous option would be vital to any mass electronic road toll proposal.

The wider availability of encryption technology also offers the possibility of enhancing privacy and guaranteeing confidentiality of private communications. A technology which was formerly the sole preserve of the military and intelligence organisations is increasingly within reach of ordinary people.

Relevance of technological issues to the review

It is worth reflecting on the relevance of the pace of technological change for the review of the operation of the Privacy Act. In my view, one of the lessons to be learned is that it is necessary to avoid the Act being linked too closely to today's technology in case the law rapidly becomes meaningless as the technology changes. There is benefit in having the Act generally remain "technology neutral".

The challenges posed by technology are shared in other countries as well. The proliferation and adoption of new technology is just one aspect of globalisation. Accordingly, in moving to address technological challenges care should be taken to keep in step with emerging international approaches.

Nonetheless, we should not ignore the challenges imposed by technology. I have no wish for the Act to be perfectly "technology neutral" yet ineffective in protecting individual privacy when confronted with new technology. The desire for generic standards should not be allowed to hinder an effective response to known technological risks. This can sometimes be done by code of practice. Sometimes the Act should directly address a technological issue. In other cases special legislation is warranted.²

Information is now technically able to be moved and transformed with great rapidity. Technology has the ability to circumvent some traditional administrative controls. Obviously new and appropriate technical and administrative controls must continue to be applied. However, such technological challenges may mean that the *legal* controls are more important than ever. If the technology itself does not have inherent limitations as to what may be done with personal information it becomes especially important that the agency entrusted with that information constrain itself consistently with the law.

ECONOMIC CONTEXT

There are two threads running through the international approach to the protection of privacy in the light of technological challenges. The first concerns human rights. The second, economics. The economic interest in the issues is plain from the fact that two of the main international "regulators" are the Organisation for Economic Cooperation and Development and the European Union.

Origins of OECD interest

As previously outlined, many developed countries began legislating to protect privacy during the early 1970s. During that and the preceding period there had been a greater emphasis on individual rights and legislatures responded by enacting legal protections. It

² For example I supported the creation of a warrant process for the use of telephone analysers. At recommendation 22 I propose the same for law enforcement use of covert video surveillance.

was also a period when a number of significant studies of privacy were undertaken because of a concern about technological developments.

The principal New Zealand example of 1970s privacy legislation was the Wanganui Computer Centre Act 1976. The level of interest during this period also saw two other privacy bills before the New Zealand Parliament to address privacy, the Preservation of Privacy Bill 1972 and the Privacy Commissioner Bill 1975. Sixteen years were to elapse before a resurgence of interest in privacy saw two further bills before Parliament.

A broad variety of national privacy laws was perceived as an economic problem by the OECD. In the Preface to the OECD Guidelines in 1980 it stated:

“The development of automatic data processing, which enables vast quantities of data to be transmitted within seconds across national frontiers, and indeed across continents, has made it necessary to consider privacy protection in relation to personal data. Privacy protection laws have been introduced, or will be introduced shortly, in approximately one-half of OECD member countries to prevent what are considered to be violations of fundamental human rights, such as the unlawful storage of personal data, the storage of inaccurate personal data, or the abuse or unauthorised disclosure of such data.

“On the other hand, there is a danger that disparities in national legislations could hamper the free flow of personal data across frontiers; these flows have greatly increased in recent years and are bound to grow further with the widespread introduction of new computer and communications technology. Restrictions on these flows could cause serious disruption in important sectors of the economy, such as banking and insurance.

“For this reason OECD member countries considered it necessary to develop Guidelines which would help to harmonise national privacy legislation and, while upholding such human rights, would at the same time prevent interruptions in international flows of data. They represent a consensus on basic principles which can be built into existing national legislation, or serve as a basis for legislation in those countries which do not yet have it.”

The OECD emphasised two economic considerations which might be characterised as follows:

- *globalisation* - a recognition of the increasing interaction of countries through the transborder flow of personal data;
- *harmonisation* - the notion that consistent legislation based upon shared principles could diminish interruptions in trade while ensuring that human rights are protected.

The Council of Europe’s 1981 Convention No 108 was similarly motivated although that body was more steeped in the human rights tradition than the OECD. The OECD Guidelines and Convention No 108 provided the framework for most general data protection or information privacy laws since enacted.

Globalisation and harmonisation

The economic considerations which drove the OECD in 1980 have not diminished. Indeed they have become more profound. The transborder data flows with which the OECD group of experts were familiar in 1980 have multiplied in quantity and type. The world that we now live in, or are heading towards, is sometimes referred to as the “Information Society” - an updated version of the 1960s “global village”. The growth of the Internet, and its potential to reshape the way business and leisure are conducted, is a notable current example.

Many jurisdictions without data protection or information privacy laws, or with limited sectoral laws, have been contemplating enacting more broadly based laws because of globalisation. Typically such governments are driven by the prospects of electronic commerce. For example, the State of Victoria in Australia has announced its intention to legislate for a privacy law as part of its policy to build a network and knowledge based economy. The discussion paper released by the Minister for Information Technology and Multimedia explains that:

“The Victorian data protection regime will provide a strategic response. It will bolster business and consumer confidence in on-line transactions by committing to a minimum standard of data protection, as expressed in the Federal Privacy Commissioner’s *National Principles for the Fair Handling of Personal Information*. These principles directly address concerns about information privacy and security. Businesses will be certain that the standards they meet will be in line with national and international expectations and consumers will be able to seek redress should the standards not be met.”³

The quotation also emphasises the common wish amongst governments to legislate for privacy consistently with national and international standards. Federal countries such as Australia and Canada fear that a patchwork of laws will increase compliance costs while failing to adequately protect privacy.

EU Directive on Data Protection

Harmonisation was also one of the principal drivers of the most significant development since 1981 - the EU Directive on Data Protection of 1995. That Directive requires EU states to bring existing laws up to the minimum standard by October this year. It seeks to impose a maximum standard of privacy protection as well.

The EU Directive’s controls on transborder data flows discussed in detail later in this report,⁴ is an economic consideration for “third countries” such as New Zealand. Indeed, this has been one of the main points of discussion since 1990 when the draft Directive was first released. From October 1998 onwards EU states will impose data export controls. European and multinational corporations which are involved in sending data to third countries for processing on an ongoing basis will have to weigh up who they can or may send personal data to.

Uncertainties as to whether a jurisdiction offers “adequate protection” bring costs for businesses yet may offer comparative advantages for jurisdictions in which adequate protection is known with certainty. In this respect the enactment of the Privacy Act in 1993 was designed to bring New Zealand agencies some comfort. Hong Kong, especially dependent upon trade, passed a similar law in 1995. A list of jurisdictions which have enacted general privacy laws, some in response to the EU Directive, since 1992 is set out at Appendix C. One can contrast the secure position of businesses in New Zealand and Hong Kong with the somewhat uncertain position of counterparts in Canada and Australia.

Public sector reform

Public sector reform has been a feature of developed countries since 1980. Reforms have been driven by various objectives including a drive for efficiency and perceived economic benefits. Privacy expectations have sometimes been a barrier to change. Typically the public sector reforms at issue have involved a function of handling of sensitive personal information being transferred to the private sector by way of outsourcing or privatisation. In some cases governments have foregone reform in particular circumstances. In other cases, governments have expressly addressed privacy concerns when making reforms.

³ State Government of Victoria, *Information Privacy in Victoria: Data Protection Bill*, discussion paper, July 1998, page 8.

⁴ See paragraph 2.8.12.

For example, Australia’s Privacy Act principally applies just to the Commonwealth public sector. Accordingly, when the present government sought to involve the private sector more closely in managing unemployment services, it needed to enact complex extensions of the Privacy Act to the relevant entities. A further bill to extend the Australian Privacy Act in response to moves to outsource a wide variety of information processing is before the Commonwealth Parliament.⁵

Prior to the enactment of the Privacy Act 1993 New Zealand had similar experiences. The Health Amendment Act 1988, and related amendments to the Hospitals Act and Area Health Boards Act, specifically crafted a privacy regime to take account of the privatisation of the health computer system. In the early 1990s a proposal to sell the Government Computing Service, which operated the Wanganui Computer Centre, was not seen as feasible in the absence of a general privacy law. The sale was postponed until after the enactment of the Privacy Act.

The existence of a seamless Privacy Act covering public and private sectors enables governments to take the decisions that they consider appropriate for the economy. That does not mean to say that governments ought to outsource or privatise particular functions carried out in the public sector, or ought not to do these things, merely that the Act provides privacy protection whether or not they do so. A range of choices, satisfactory from a privacy perspective, remain available to any government.

Another aspect of economic concern of government has been a wish to avoid the imposition of excessive compliance costs on businesses. The Privacy Act is a product of a desire to protect privacy adequately while, at the same time, avoiding significant administration costs for the Government or undue compliance costs on business. A significant step was taken in this regard with the study of comparative jurisdictions in *Data Privacy: An Options Paper* prepared for the Minister of Justice in 1987. That report offered clear warnings against the licensing and registration systems used in Europe and steered the Act towards a more “light handed” approach. The decision to apply the law equally to public and private sectors, and not to distinguish between automatically processed and other information, has avoided many of the complexities, demarcation problems, inconsistencies and ineffectiveness, of some overseas laws. Furthermore, the detailed study of the Privacy of Information Bill by a select committee led to a series of significant changes, many of which were directed towards minimising compliance costs.

Economic considerations in the review

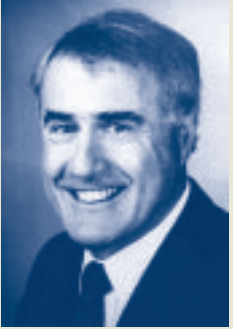
Section 14(a) directs me in to have due regard for, amongst other things, social interests that compete with privacy including the general desirability of a free flow of information and the recognition of the right of government and business to achieve their objectives in an efficient way. I have carefully taken into account a variety of the economic considerations as I have undertaken this review. In particular, I have sought to:

- be alive to those features of the Act which were intended by the Government, or the Select Committee, to ensure that the Act operated in an efficient and satisfactory way and to review and if necessary enhance those features;
- consider ideas for minimising compliance or administration costs while effectively protecting privacy;
- examine the emerging international approach to transborder data flows and to consider whether any change to our Act is warranted;
- ensure that the Act provides “adequate protection” in terms of the standards in the EU Directive on Data Protection.

LEGISLATIVE HISTORY

Introduction

While there are many features in the Privacy Act without precedent in New Zealand legislation, the Act also represents a consolidation and evolution of a number of earlier



Rt Hon Geoffrey Palmer:
Commissioned the 1987
*Data Privacy: Options
Paper* which shaped
subsequent information
privacy initiatives.

PHOTO: ALLAN JENKINS



Tim McBride: Author of
the 1984 *Privacy Review*
and 1987 *Data Privacy:
Options Paper*.

PHOTO: OFFICE OF THE
PRIVACY COMMISSIONER.

⁵ Privacy Amendment Bill 1998 (Australia).

legislative initiatives. The Act also contributes to implementing New Zealand’s international obligations.

Features of the Privacy Act which represent a continuation of the existing New Zealand statutory tradition include:

- vesting in the Privacy Commissioner functions formerly carried out by the Wanganui Privacy Commissioner, Human Rights Commission, Ombudsmen and Information Authority;
- continuing access rights formerly contained in the Wanganui Computer Centre Act 1976, Official Information Act 1982 and Local Government Official Information Act 1987;
- consolidating aspects of the Wanganui Computer Centre Act 1976, Health Amendment Act 1988 and related health sector legislation, and the Privacy Commissioner Act 1991.

The legislation directly implements the OECD Guidelines which New Zealand accepted in 1980. It also represents a measure to protect people from arbitrary interference with their privacy and to provide a remedy for any such interference. New Zealand assumed such obligations when it signed the International Covenant on Civil and Political Rights in 1968 and later ratified it in 1978.

In the following material I outline some of the influences which have helped to shape our legislation. I mention some of the previous bills, statutes, official reports and processes of relevance. The material should be read together with Appendix D which lists many of the key influences since 1972 and Appendix H, which lists provisions in earlier statutes upon which the Act is based.

It should be plain from the material that the Act is not a “bolt from the blue”. It is the outcome of many years of study of the issues informed by forays into legislation covering particular computer databases and sectors and governing access to information. The Act’s complaints resolution processes draw upon well tested and successful models pioneered in New Zealand since 1962 in the Ombudsman Act and adapted in 1977 and 1982 for discrimination complaints and information access reviews.

The 1970s - Experimental national legislation

Many countries began legislating to protect privacy from the early 1970s as a response to concerns about the effects of modern technology on individuals. The first privacy bill brought before the New Zealand Parliament was the Preservation of Privacy Bill introduced in 1972 by Squadron Leader Drayton MP. Mr Drayton’s bill ran to just 22 clauses. It would have established a Privacy Commissioner to be the registrar of all computer installations in New Zealand. The owners of computer installations would have been obliged to supply a copy of any information programmed into the computer system to the individual concerned within three months. Thereafter the individual could obtain a printout on request.

As is common with private members’ initiatives the Preservation of Privacy Bill was defeated on its introduction. However, some points of interest may be noted:

- the Parliamentary debate shows bipartisan concern about privacy and the challenges posed by computer databanks - which foreshadows the fact that both a new Labour, and a subsequent National, government were to propose legislation within four years;
- this was the only New Zealand bill ever to propose registration of computer systems - registration has never found favour here notwithstanding its adoption in the UK and throughout Europe;
- this bill initiated the use of “privacy” in preference to the European term “data protection” and was the first to propose a “Privacy Commissioner” - features found in every subsequent bill.

The first Government privacy bills also appeared in the earlier 1970s. The Private Investigators and Security Guards Act 1974 might be counted as the first tentative step since



Squadron Leader Drayton MP: Introduced the first privacy bill to the New Zealand Parliament in 1972.

PHOTO: ALLAN JENKINS



Hon Dr Martyn Finlay: Minister of Justice responsible for the introduction of New Zealand’s first Government bill to establish a Privacy Commissioner. The Privacy Commissioner Bill 1975 did not survive the subsequent change of Government.

PHOTO: ALLAN JENKINS



Hon Arthur Faulkner: Minister of State Services responsible for introducing the Wanganui Computer Centre Bill in 1975. This pioneering law was notable for being both New Zealand's first data protection law and its first freedom of information law.

PHOTO: ALLAN JENKINS



Hon David Thomson: As Minister of Justice oversaw the creation of the Human Rights Commission which had, amongst its other responsibilities, an inquiry function in respect of privacy.

PHOTO: ALLAN JENKINS



Hon Peter Gordon: As the new National Minister of State Services, John Gordon was responsible for the enactment of the Wanganui Computer Centre Act 1976, introduced by the previous government.

PHOTO: ALLAN JENKINS

its long title made it clear that it was intended to afford “greater protection to the individual’s right to privacy against possible invasion by private investigators”. However, two bills introduced in 1975 fall more clearly into the mainstream of information privacy initiatives. These were the Privacy Commissioner Bill, introduced by Hon Dr A M Finlay, Minister of Justice, and the Wanganui Computer Centre Bill, introduced by Hon A J Faulkner, Minister of State Services.

The Privacy Commissioner Bill would have established a Privacy Commissioner with an inquiry and reporting function but without a complaints jurisdiction. In this respect, it has much in common with the bill which bore the same name in 1991. In the words of Dr Finlay:

“The Commissioner will act as a sounding board and gather information in the field of privacy with the ultimate object of assisting Government departments decide what, if anything, needs to be done in the way of legislation or otherwise.”

It was also anticipated that further functions would be conferred upon the Privacy Commissioner by other legislation including, in the first instance, under the Wanganui Computer Centre Bill.

The Privacy Commissioner Bill did not survive a change of government in 1975. The new National Government instead conferred a limited privacy jurisdiction, again excluding complaints, upon the Human Rights Commission established in 1977. However, the Wanganui Computer Centre Act 1976 was enacted into law. Amongst other notable features that Act established:

- New Zealand’s first Privacy Commissioner;
- New Zealand’s first freedom of information law with the Commissioner operating a bureau enabling individuals to have access to information held about them on the computer;
- institutional and legal controls to protect privacy in the face of the large new computer databank.

During the 16 years of the 1976 Act’s operation four persons were to hold the post of Privacy Commissioner (see Appendix D). Sir George Laking was the first Commissioner. He relinquished the post as the administrative load became too much given his combined role as Ombudsman. Amongst other things, Sir George established systems to enable individuals to obtain access to their criminal history information. Mr R A (later Justice) McGechan, then Deputy Chairman of the Wanganui Computer Centre Policy Committee, temporarily served as Commissioner until Sir James Wicks commenced a five year term in 1978. During his period as Commissioner, but separate from those tasks, Sir James was to chair the Committee of Inquiry into the Administration of the Electoral Act following registration difficulties associated with the 1981 election. Paul Molineaux was to serve two five-year terms as Wanganui Commissioner starting in 1983. In the event, Mr Molineaux was to be the last such Commissioner appointed under the 1976 Act sharing the last year of his appointment as Wanganui Computer Centre Privacy Commissioner with my first year as Privacy Commissioner under the Privacy Commissioner Act 1991.

The 1980s - International standard setting, local study and sectoral legislation

The 1976 Act was hailed as a world class data protection and freedom of information measure. However, on both counts the law soon became outclassed. A far more sophisticated approach to data protection was expected following the OECD Guidelines (1980) and Convention No 108 (1981) while much more extensive freedom of information legislation was enacted in New Zealand in 1982. The Wanganui Computer Centre Privacy Commissioner endorsed calls for new, more comprehensive, privacy legislation describing the existing law in his 1989 annual report as “piecemeal, fragmented and incomplete”.

In addition to the OECD and Council of Europe standard setting at international level, there were a variety of privacy studies undertaken in the 1980s. For example, in New Zealand the 1984 *Privacy Review*, prepared pursuant to the Human Rights Commission Act 1977, provided a resource for the promotion of debate about privacy.

Across the Tasman, the Australian Law Reform Commission published its two volume *Privacy* report. The 1983 report was one of the most comprehensive ever on the subject of information privacy. The Australian Commission was headed by Justice Michael Kirby, who had earlier chaired the OECD Group of Experts which drafted the OECD Guidelines, and had amongst its researchers Kevin O'Connor, later to become Australia's first Privacy Commissioner. The Commission proposed a draft privacy bill, parts of which formed the basis of the Australian Privacy Act 1988. The Australian Act was a model from which the New Zealand Act was to heavily borrow.

The access and correction provisions in the Act were to be derived in large measure from the Official Information Act 1982, which was itself based upon recommendations of the Committee on Official Information (“the Danks Committee”). A similar committee, chaired by Sir Alan Danks, was constituted as the “Information Authority” pursuant to the 1982 Act. The Information Authority functioned for five years before going out of existence.

In 1985 the Information Authority released a discussion paper concerning personal information and the Official Information Act. In 1987 it followed with a further discussion paper putting forward recommendations for reform to address information privacy concerns. The paper suggested principles to govern the collection and use of personal information and proposed clauses which could be included in the Official Information Act. The process finally led to a 1988 report to Parliament on the subject of the collection and use of personal information.⁶ The report was not implemented in the fashion recommended but was undoubtedly an influence upon the later drafting of the Privacy of Information Bill.

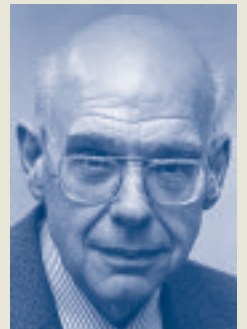
The Information Authority report was released at the time of the privatisation of the health computer system. As a result, amendments were made to the Health Act, Hospitals Act and Area Health Boards Act, to craft a privacy regime governing the collection, holding, use and disclosure of personal information consistent with aspects of the Information Authority's report. In addition to the more usual security obligations, access and disclosure constraints, the amendments might be considered the first provisions in New Zealand's law implementing the OECD collection limitation principle. The 1988 health sector privacy legislation was repealed in 1993.

The Broadcasting Act 1976 was a further piece of specific sector privacy legislation. That Act required programme standards to be consistent with the privacy of the individual and enabled complaints to be taken to the Broadcasting Tribunal. This was carried forward into the Broadcasting Act 1989 which also provided for compensation for privacy complaints, unlike other breaches of standards. The existence of that provision is relevant to the debate over the significance of the exemption from the Privacy Act of the news media in their news activities. Unlike the print media, there are privacy standards applicable to the broadcast media under which complaints may be brought and compensation obtained.

The 1990s - Comprehensive privacy legislation

Prior to the 1990 election officials had already undertaken preparatory work to draft information privacy legislation. This work followed through on the 1987 *Data Privacy: An Options Paper* and the 1988 Information Authority report. It may also have been in contemplation of government data matching.

⁶ Information Authority, *Report of the Information Authority on the Subject of Collection and Use of Personal Information*, May 1988.



Sir Alan Danks: Chaired the Committee on Official Information which recommended the repeal of the Official Secrets Act 1951 and the enactment of the Official Information Act. Sir Alan went on to chair the Information Authority which recommended enactment of a law governing collection and use of personal information.

PHOTO: NORTHERN ADVOCATE



Hon Jim McLay: Minister of Justice responsible for the enactment of the Official Information Act 1982 in the final term of the Muldoon government.

PHOTO: ALLAN JENKINS

By the time of the 1990 election both major parties were committed to information privacy legislation. The change in government led to a delay in the public production of a bill. As a spur to action, the opposition Labour Party introduced its own bill in the name of Peter Dunne MP. Peter Dunne's Information Privacy Bill 1991 was followed in the same year by the new National Government's Privacy of Information Bill. The two bills were very similar except the Dunne Bill proposed to continue the function of the Wanganui Computer Centre Privacy Commissioner to act as a bureau for releasing information to individuals from the Wanganui Computer Centre.

Both bills were referred to the Justice and Law Reform Select Committee. The bills stirred a degree of controversy and attracted quite a number of submissions. Only the Government bill progressed.

One of the prime objectives of the Government bill was to authorise and regulate a government data matching which was referred to as "information matching" based upon a similar Australian law passed the previous year.⁷ The tackling of welfare fraud was a plank in the Government's 1991 social welfare reforms and so it did not wish to see significant delay in the introduction of information matching. However, it was plain that the privacy bills would require a great deal of study and consultation. The Government took the decision to split off from the Privacy of Information Bill those parts establishing a Privacy Commissioner and governing information matching and enact them separately from the rest of the bill.

Accordingly, the Privacy Commissioner Act 1991 was enacted in December 1991 just four months after the Privacy of Information Bill had been introduced without the Select Committee having studied the balance of the bill. This was a controversial move. The Opposition voted against the 1991 Act.

The Select Committee studied the proposals for information matching and made significant changes to the bill. In particular, information matching programmes were no longer to be authorised by the Privacy Commissioner but instead by legislation. The Commissioner was to have a reporting and oversight role but not, at this stage, a complaints function. Concern was expressed as to how effective such a Commissioner could be. The Government's position was that this was a temporary arrangement pending Parliamentary consideration of the balance of the Privacy of Information Bill.

The Select Committee continued its study of the Privacy of Information Bill during 1992 and early 1993. Having heard submissions, a great deal of change was proposed. In conducting this work the Committee was to have my assistance as the first Privacy Commissioner appointed under the 1991 Act. I used the opportunity to familiarise myself with privacy issues and to meet with many of the organisations which had expressed concerns about the bill in their submissions. The Committee acknowledged it was greatly assisted by Margaret Nixon of the Department of Justice and by Geoff Lawn of the Parliamentary Counsel Office.

Amongst notable changes made to the bill, the Select Committee:

- provided for codes of practice to be issued by the Privacy Commissioner;
- introduced an exemption for the news media and members of Parliament;
- created special controls on public register personal information;
- dropped some of the information privacy principles from the bill but created a new one concerning unique identifiers;
- permitted private sector agencies to charge for access.

The Select Committee's work was accelerated as it became apparent that it would be desirable for the Privacy Act, as the bill was now to be known, to be in place in time for the public sector health reforms due to begin in the middle of 1993. It was recognised that there would be public concerns about the protection of sensitive health information as a result of those reforms.



Peter Dunne MP:
Introduced the Information Privacy Bill 1991. This Opposition initiative spurred further interest in the issue and set the scene for eventual bipartisan support for the enactment of the Privacy Act.

PHOTO: P DUNNE



Rt Hon Douglas Graham:
Minister of Justice responsible for the introduction of the Privacy of Information Bill. While the bill was initially controversial, the Minister guided the Privacy Act 1993 to eventual enactment with unanimous Parliamentary support.

PHOTO: WOOLF LTD

⁷ Data-matching Program (Assistance and Tax) Act 1990 (Australia).

Some reflections on legislative history

The bill was passed through Parliament on 5 May 1993 and received Royal Assent 12 days later. The Privacy Act consolidated the limited 1991 legislation and produced a privacy law more comprehensive than any outside Europe. The Select Committee had done such a careful job of addressing concerns that had been raised in submissions on the bill and in Parliament during the enactment of the Privacy Commissioner Act 1991 that it was finally passed with complete bipartisan support.

In undertaking the review of the Privacy Act I have been conscious of what has gone before. My overall view of the Act is that it is well conceived and approaches the task in an appropriate manner. Naturally, there is room for improvement. Indeed, I have made over 150 recommendations. However, a study of our legislative history, and that of other similar jurisdictions, suggests to me that the Act is indeed firmly on the right track.



Hamish Hancock MP:
Responsible, as Chair of the Subcommittee of the Justice and Law Reform Select Committee, for studying the Privacy of Information Bill and recommending changes to the renamed Privacy Act 1993.

PHOTO: H HANCOCK

Part I

Preliminary Provisions

I

“Good, functional typography and design are invisible. Good design allows readers to concentrate their energy on substance rather than be distracted by format. A bad design remains a bad design, even though it may be redeemed to some extent by familiarity.”

- Law Commission, *The Format of Legislation*, 1993

“The Privacy Act’s accommodation of the concurrent needs for flexibility and certainty appears to have been bought at the price of simplicity.”

- Dr Paul Roth, preface to *Privacy Law and Practice*, July 1994

“The bill continues to cover the public and private sectors. There are exemptions and partial exemptions that are suitable now but it is intended that they be re-examined as time goes on. I am referring to the provisions on members of Parliament, the Parliamentary Service Commission, the Parliamentary Service, the news media, and the intelligence agencies. The bill gives power to the Privacy Commissioner to review the Act after 3 years, then at intervals of 5 years. The consequence of these reviews should be gradually to bring within the scope of the law those bodies I have listed, given the importance to them of the proper handling of personal information”.

- Hon Douglas Graham (Minister of Justice) on the Second Reading of the Privacy of Information Bill, April 1993

1.1 INTRODUCTION

1.1.1 Part I sets out preliminary provisions. Section 2 (interpretation) defines terms used throughout the Act. The definition of “agency” largely determines the scope of the Act’s application.

1.1.2 In this part of the report I comment upon sections 1-5 and where appropriate offer recommendations for amendment. Before moving to the section by section analysis I will address general style and drafting issues.

1.2 DRAFTING STYLE

Introduction

1.2.1 I hold the skills of the Parliamentary Counsel Office, which drafts New Zealand legislation, in high regard. The skill exercised in preparing such a ground breaking piece of legislation is evident throughout the Act. That the Act achieves the tasks set for it in a legally effective and appropriate manner is, in my mind, in no doubt. The provisions in the Act work very effectively by and large. It has not brought the problems predicted by long-standing opponents of indi-

vidual privacy rights. Credit in this respect is also due to the Justice and Law Reform Committee which studied the Privacy of Information Bill with such care and recommended significant amendments.

- 1.2.2 The Parliamentary Counsel Office and the select committee built upon established precedents which themselves had been prepared with great skill. The OECD Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data were of particular importance on a conceptual and policy level. In terms of the structural and drafting issues, the Privacy Act 1988 (Commonwealth of Australia), the Official Information Act 1982 and the Ombudsmen Act 1975 were heavily drawn upon.
- 1.2.3 Nonetheless I am bound to say that the Act has not won universal acclaim for the simplicity of its drafting. In the course of the review, many people expressed to me a hope that aspects of the drafting and style of the Act could be simplified. It is appropriate that I give prominence to this issue at the outset of the Part by Part, section by section, discussion of the Act.
- 1.2.4 Lest there be any misunderstanding, I must add that criticism of the drafting or style of the Act is not universal, nor always deserved. Indeed, many regular users of the Act express a large measure of satisfaction. As agencies come to understand the law they often see it as appropriate, relatively straightforward and easy to use, and without significant shortcomings. The group of people who have the most difficulty with the Act are those who are not familiar with working with statutes.
- 1.2.5 Since the Privacy Act applies to such a wide range of agencies in the public and private sectors it is desirable that the Act be as “user friendly” to ordinary people as possible. If ordinary users of the Act within agencies are daunted from reading, and seeking to understand, the provisions of the Act there are risks that they will:
- continue with unfair information handling practices in a “business as usual” mode;
 - not base their decisions on the Act’s provisions but upon what other people tell them the Act requires - which may be wrong;
 - feel compelled to seek legal advice, with attendant costs, for what should be able to be readily ascertained by reading the legislation itself.
- 1.2.6 Various people have suggested to me that the Act could be rewritten in what they believe to be a clearer and more succinct style. It is conceivable that clearer structure and drafting could be achieved in a rewritten Act at comparable length to the present statute. However, I advise against attempting a major rewrite. A number of submissions emphasised the point, already apparent to me, that users of the Act have become familiar with the statutory structure and provisions and that wholesale change would provide an unwelcome disruption. It could also lead to uncertainty as to whether the changes are of substance or style.
- 1.2.7 However, there is scope to enhance the drafting and style of the Act while causing those familiar with the Act little disruption. In that light my recommendations on drafting style are premised upon there being no wholesale change to the section numbers presently in use. I have not lightly recommended splitting, switching, renumbering or reordering sections.
- General statutory format*
- 1.2.8 The format and presentation of New Zealand statutes is not too different from that in place at the time of the 1908 consolidation. Very little about our legislation appears “modern” whether one considers the page size, indentation, punctuation, use of capital letters, numbering, headings or a variety of other matters. The Privacy Act therefore has an unfamiliar “feel” about it for lay people

“The legislation is complex, lengthy and is not readily understood.”

- NZ BANKERS’ ASSOCIATION,
SUBMISSION S25

used to modern layouts, a range of font types, effective headings and such like in other documents they use. Anyone can achieve presentations in desktop publishing which, just a few years ago, were the preserve of typesetters and professional printers. The public, not unreasonably, now expect official publications to be presented in a clear and modern format from which they can easily locate the information that they need. This is not always the case with the Privacy Act.

- 1.2.9 While “ignorance of the law is no excuse” one can have sympathy for, say, a manager versed in business documents who possesses a copy of a statute yet cannot find the relevant passage or, when he or she does so, cannot understand it. Australia and Canada have modernised the presentation of their statutes beyond anything so far attempted here. The “office consolidations” produced in Canada even come with an index. The hypothetical business person would have a greater degree of confidence in using that legislation.
- 1.2.10 Big changes for the format, structure and style of New Zealand legislation have been proposed by the Law Commission and some aspects of these have been adopted, or are under study, by the Parliamentary Counsel.¹ I wish them well but turn to more modest reforms that I believe can be achieved in one statute, the Privacy Act. In making these recommendations I acknowledge that there is no “magic bullet” to turn a statute which has an old fashioned and complex look into a modern appearing, and simple to use, document.
- 1.2.11 Having ruled out recommendations which would significantly alter the familiar structure and numbering of sections, the format and style recommendations that I make are modest. However, within such constraints, I believe that changes could:
- rid the Act of some old fashioned aspects which discourage non-lawyers - the use of “shall”, Roman numerals, etc;
 - assist users to locate particular information within the text - through an enhanced analysis (list of contents) and marginal notes (headings);
 - direct users more effectively to other relevant statutes through reform of the section notes;
 - make some of the Act’s provisions easier to understand.
- 1.2.12 I approach the issues in the following order:
- adoption of Parliamentary Counsel Office changes in drafting style;
 - amendment to marginal notes;
 - consolidation of endnotes;
 - planning for a consolidated reprint;
 - noting other relevant recommendations.

Parliamentary Counsel Office changes in drafting style

- 1.2.13 The Parliamentary Counsel Office announced seventeen changes in its drafting style from 1 January 1997.² I have studied the changes and have concluded that six of them have some particular relevance to the Privacy Act. In Appendix E I have noted the six changes and added my own comments in respect of the Privacy Act. Briefly the proposed changes, and the relevance for the Privacy Act, are:

1. Dropping “of this Act” etc: This will make for shorter cross references within the Act as there would be scores, if not hundreds, of instances in the Privacy Act where the phrase “of this Act”, “of this section”, “of this subsection” or “of this principle” appear.

¹ See Law Commission, *The Format of Legislation*, 1993, and *Legislation Manual: Structure and Style*, 1996. I have adopted a more modern style in codes of practice than found in legislation. In doing so I have followed many of the Law Commission’s recommendations.

² See Parliamentary Counsel Office, *A Guide to Working with the Parliamentary Counsel Office*, September 1997.

2. Numbering parts in Arabic instead of Roman: The twelve Parts of the Act are currently identified by Roman numerals. The Second Schedule is similarly divided in this manner.
 3. Numbering schedules 1, 2 instead of First, Second: The Privacy Act’s eight schedules are currently labelled in the older manner.
 4. Alternatives for “shall” in appropriate cases: The Privacy Act uses “shall” in numerous instances. Each of the twelve information privacy principles uses the word “shall” at least once. Principle 7 uses “shall” five times. “Must” and “is to” are often satisfactory alternatives.
 5. Drop unnecessary “except as provided”, “subject to”, and “notwithstanding” formulations. These formulations appear in the Privacy Act at various places.
 6. Include further material in the analysis: The present analysis does not list the Act’s twelve information privacy principles, four public register privacy principles or eight schedules.
- 1.2.14 Of those changes, the most beneficial may be the simplest - listing the principles and schedules in the analysis. This will enhance the ability of users of the Act to locate relevant information. The other changes would be barely perceptible individually but taken together would mark an improvement in the style and appearance of the Act by:
- making it briefer in places - changes 1 and 5;
 - making the appearance more modern - changes 2, 3, 4, and 5;
 - making it more understandable to laypeople - changes 2, 4 and 5.
- 1.2.15 The Parliamentary Counsel Office has commenced a process of modernising and changing the drafting style in legislation. This is not something that can be achieved overnight and might not normally be attempted in an existing Act. I prefer that the unusual step be taken of introducing stylistic amendments throughout the text of the Privacy Act.³ If practicable I believe that the attempt should be made to adopt the modern format given the statute’s widespread applicability to a range of agencies.



RECOMMENDATION 1

The relevant changes in legislative drafting styles recently adopted by the Parliamentary Counsel Office should be applied throughout the Privacy Act.

Marginal notes and headings

- 1.2.16 Some of the marginal notes and headings have been found to be unhelpful, unduly technical or even misleading. The following changes are suggested:
- principle 9: “Agency not to keep personal information for longer than necessary” change to “Retention of personal information”;
 - section 7: “Savings” change to “Saving of effect of other laws” or “Effect of other laws on information privacy principles”;
 - section 27: “Security, defence, international relations, etc” change to “Security, international relations, maintenance of the law, safety, etc”;⁴
 - section 28: “Trade secrets” to “Trade secrets and prejudice to commercial position”;
 - section 42: “Documents” change to “Ways of making information available”;

³ My preference would be for the resultant reprint not to be cluttered with bold brackets highlighting changes which are purely stylistic. Otherwise some of the changes may increase rather than diminish clutter.

⁴ This change will be superseded if my recommendation to split the reasons for withholding into separate sections is adopted. See recommendation 47.

- section 45: “Precautions” change to “Precautions when giving access” or “Precautions concerning identity of requester or agent”;
- section 73: “Proceedings of Commissioner” change to “Parties to be informed of investigation”;
- section 95: “Disclosures of information, etc” change to “Disclosures of secret information, etc”;
- Part X: “Information matching” change to “Authorised information matching programmes”;⁵
- sections 100, 101 and 105: insert the word “authorised” before the phrase “information matching programme”;
- information matching rule 8: “Time limits” change to “Annual frequency of matching”.

- 1.2.17 The present heading of principle 9 has caused misunderstandings. The principle does not literally state that an agency is not to keep personal information for “longer than necessary”. Rather, it prohibits keeping information for “longer than is required for the purposes for which the information may lawfully be used”. A simple reference to “retention of personal information” in the heading may suffice to avoid confusion.
- 1.2.18 Section 7 needs to be found by any user of the Act who is to obtain a full appreciation of how the law works. Unfortunately, the special use of the word “savings” is not widely understood by non-lawyers. It is also used elsewhere in the Act (section 132). The alternatives of “saving of effect of other laws” or, preferably, “effect of other laws on information privacy principles” will direct the user of the Act to the relevance and importance of the provision more clearly.
- 1.2.19 The section 27 marginal note, taken directly from the Official Information Act, obscures the fact that the section includes two of the most important grounds for withholding information relating to the maintenance of the law and the endangering of the safety of any individual. Instead, attention is directed to security, defence and international relations, which are relevant to only a tiny proportion of access requests. The suggested change will downplay defence and emphasise the maintenance of the law and personal safety. The section 28 marginal note, trade secrets, presently describes only the first of alternative grounds for refusal of a request.
- 1.2.20 In sections 42 and 45 respectively, the marginal notes “documents” and “precautions” are taken from the Official Information Act which is a shorter statute dealing almost exclusively with access issues. In the wider scope of an information privacy law it is desirable to direct attention to the fact that the “documents” clause concerns the ways of making information available and “precautions” relates to precautions to be taken when giving access to verify the identity of a requester or agent.
- 1.2.21 The marginal note for section 73, “Proceedings of Commissioner”, is unfortunate since it conveys very little information and duplicates headings or subheadings used in Parts VIII and IX. A more informative note would be “Parties to be informed of investigation”. Similarly, the marginal note to section 95, “Disclosures of information, etc”, is too broadly stated for a general information privacy law. “Disclosures of secret information, etc” will better capture the effect of the section.
- 1.2.22 The heading to Part X should be changed to “*Authorised* information matching programmes”. Part X is not widely known or understood and confusion arises when agencies believe that Part X applies to them when in fact it does not. *Authorised* will make clear that the Part’s primary focus. Reference to *programmes* will emphasise the schemes being regulated.

⁵ A proposal to style “information matching” as “data matching” is canvassed at recommendation 119.

“There needs to be increased use of definitions as per Discussion Paper 1. As the Act has major impacts for, and is there to protect individuals and enhance privacy, the use of Plain English is imperative if they are to understand and use it. References to other Acts are couched in language which is often difficult for non-legal people to understand.”

- WELLINGTON CITY COUNCIL,
SUBMISSION WX5

- 1.2.23 Sections 100, 101 and 105 each concern “*authorised* information matching programmes” rather than the broader category of “information matching programmes”. The marginal notes should reflect this. Information matching rule 8 refers to “time limits” whereas it is more concerned with the frequency of matching.



RECOMMENDATION 2

The marginal notes and headings in the following principle, sections, Part and rule should be amended to make them more helpful, accurate and precise: principle 9; sections 7, 27, 28, 42, 45, 73, 95, 100, 101 and 105; Part X; information matching rule 8.

Section notes and endnotes

- 1.2.24 The published Act contains a variety of notes at the end of each section (referred to as section notes) and at the end of the Act (endnotes). The Law Commission has suggested more extensive use of statutory notes. The recent changes in drafting style adopted by the Parliamentary Counsel Office do not alter the use of notes. If the position changes it will be valuable to explore the inclusion of additional notes to enhance understanding of legislation.

- 1.2.25 However, in the absence of any general change I direct my remarks solely to existing notes. The only endnote is that the Act is administered in the Department of Justice (which, on reprinting, would show the *Ministry* of Justice). The existing section notes cross refer to other Acts on which the legislation is based. These are:

- the Privacy Commissioner Act 1991;
- the Privacy Act 1988 and the Data-matching Program (Assistance and Tax) Act 1990 (Australia);
- the Data Protection Act 1984 (UK); and
- the Ombudsmen Act 1975, the Human Rights Commission Act 1977, the Official Information Act 1982 and the Local Government Official Information and Meetings Act 1987.

- 1.2.26 The Law Commission advises:

“Consider the practical value of the information before including a note. Do not allow a multitude of not very helpful references to some outdated statute to interrupt the flow and interfere with the appearance of an enactment. For example, it may be preferable to present a comparative table at the end of the Act rather than to give a note after each section.”⁶

- 1.2.27 There is definite value in having references to the official information legislation since this can direct users to secondary sources of interpretation of the sections and encourage consistent application of identical provisions. However, section notes do not convey full comparative information. For example, section 29 is followed with this endnote:

“cf. 1982, No.156, ss.18(c)(ii), (e), (g), (h), 27(1)(b) - (h), (2); 1987, No. 8, s.15(1); 1987, No. 174, ss.17(c)(ii), (e), (g), (h), 26(1)(b) - (h), (2).”

- 1.2.28 This information is of little use unless one can accurately match the paragraph and subparagraph references to paragraphs and subparagraphs within the section. I think it would be beneficial to move the section notes, or at least the Official Information Act references in Parts IV and V, to the end of the statute

⁶ Law Commission, *Legislation Manual: Structure and Style*, 1996, paragraph 121.

“Probably is room for improvement in wording of the Act to make it as easily understood as possible. This would enhance compliance. Also useful within an organisation to have people with specialist skills in this area to consult.”

- NZ ASSOCIATION OF
SOCIAL WORKERS AOTEAROA,
SUBMISSION WX4

in a comparative table or tables. Furthermore, unless one has some experience in using statutes the section notes simply appear to be “gobbledygook”. Only a user familiar with the legislative history of the statute, or who has access to a full set of statutes, will realise that the section note references are to the Official Information Act 1982, the Official Information Amendment Act 1987 and the Local Government Official Information and Meetings Act 1987. However, if the information were to be tabulated with the short title of each statute given it would be straightforward for all users of the Act to trace those helpful references.



RECOMMENDATION 3

The present section notes concerning the official information legislation should be presented in a comparative table at the end of the Act.

Consolidated reprint

- 1.2.29 It is expected that there will be an amendment bill to implement changes accepted by the Government. Those amendments, taken together with other amendments made since 1993, make the Privacy Act a suitable candidate for a consolidated reprint at an early date. A consolidated statute would capitalise upon any drafting and stylistic changes adopted. It would likely also be presented in a more modern design and typography as changes to this are currently under study by a working group.



RECOMMENDATION 4

The Parliamentary Counsel Office should be requested to arrange for a consolidated reprint of the Privacy Act following the implementation of reforms adopted as a result of this report.

Recommendations elsewhere in report

- 1.2.30 Throughout this report I have kept in mind the desirability of stylistic and drafting changes which will enhance the Act’s “user friendliness” for all users and especially for people unfamiliar with this Act or statutes generally.

SECTION BY SECTION DISCUSSION

1.3 SECTION 1 - Short title and commencement

Rapid commencement

- 1.3.1 The Act obtained the Royal Assent on 11 May 1993 and came into force less than two months later. This contrasts with the Official Information Act, which commenced precisely 10 years earlier, for which over six months was allowed between Royal Assent and commencement. It would have been valuable to have had longer to prepare for the commencement of the statute. A “breathing space” would have been desired by agencies and my office alike although I did at least have the advantage of having been Privacy Commissioner since 1992 - under the Privacy Commissioner Act 1991. Among the difficulties I faced was the coincidence of the commencement of the jurisdiction with the start of the financial year. With no transitional funding, the office had to expand from a staff of two, and then three, who had been involved in the advisory, policy and monitoring roles under the Privacy Commissioner Act, to provide a full enquiries and complaints service.
- 1.3.2 Despite severe strains upon the resources of a small and newly staffed office, considerable activity was undertaken to seek to assist in a smooth implementation of the Act. In the weeks between the assent and commencement a series of fact sheets were produced. Drafted with care, they remain in use years later. At the same time, a code of practice for the health sector was issued within a month of the commencement of the Act.

“Dunedin City Council believes that generally the Privacy Act is a workable piece of legislation which is in the best interests of all New Zealanders as long as it is approached and applied with common sense.”

- IN LOCAL GOVERNMENT NEW ZEALAND, SUBMISSION S51

- 1.3.3 I have little doubt that with a longer period for preparation the implementation may have been a little smoother - especially if the funding difficulty was avoided. Nonetheless, the Act's commencement was satisfactory, due in part, I expect, to the delayed enforceability of some provisions.

Delayed enforceability

- 1.3.4 Although the Privacy Act came into force on 1 July 1993,⁷ certain provisions did not become enforceable, or fully enforceable, until 1 July 1995⁸ or 1 July 1996⁹.
- 1.3.5 The delay in implementation of the enforceability of some of the principles was intended to give agencies a chance to prepare and, if necessary, to adjust their information handling practices. All the information privacy principles applied from the first day of the Act but enforceable remedies only became available immediately in respect of four of the principles. Delayed enforceability was designed to minimise the compliance cost impact as the new regime took force. I believe it was successful in that respect.

1.4 SECTION 2 - Interpretation

- 1.4.1 Section 2 is a key provision in the Act which assists in interpreting, and applying all the other provisions in the Act. The section sets out a series of definitions which are used to give a standard meaning to words or phrases that occur frequently in the Act. As the Law Commission's *Legislation Manual* explains, definitions contained in statutes can be used to delimit, extend, or restrict the meaning of a term in common usage.
- 1.4.2 A number of submissions were made that the answer to perceived problems of interpretation was to be found in creating new statutory definitions. While paying careful heed to all submissions, I approach such suggestions with considerable caution.
- 1.4.3 Sometimes the suggestions have been made in respect of relatively common English terms with which most users of the Act have little difficulty. The few users which do have difficulty sometimes insist upon fanciful or unlikely interpretations. Normal rules of statutory interpretation can easily cope with many such misunderstandings but a problem exists that many users of the Act are not familiar with the canons of interpretation. Such problems are not necessarily solved by inserting new statutory definitions which can bring a range of interpretational problems of their own.
- 1.4.4 More definitions mean a longer statute and the possibility of more rather than less complexity. On the question of creating new definitions I have tended to favour the *status quo* unless persuaded otherwise. However, if any significant problems of interpretation can be solved through simple new definitions then the opportunity should certainly be taken to adopt such change.
- 1.4.5 Section 2(1) contains 35 definitions and subsection (2) sets out a rule of interpretation. In the period since July 1993 there have been opportunities to consider and interpret many of these definitions by my office. A limited number of the terms have been considered by the Complaints Review Tribunal.
- 1.4.6 In the discussion paper I sought comment upon any of the defined terms, not simply those I had identified for particular attention. Very few of the definitions attracted comment and most have, I understand, worked perfectly ad-

⁷ With the exception of section 31.

⁸ See section 8(4).

⁹ See sections 9 and 79.

equately. This is not surprising since most of the definitions are straightforward and many have been used in other enactments such as the Official Information Act. However, in the paragraphs that follow I comment upon a number of the terms defined in section 2(1).

Agency

- 1.4.7 The definition of “agency” is particularly important as the information privacy principles are all expressed to apply to agencies. The definition starts out all-encompassing (a person or body of persons whether corporate or unincorporate and whether in the public sector or private sector) but continues with 13 exceptions. Accordingly, the series of exceptions are particularly important since they determine the overall scope of the Act.
- 1.4.8 Broad coverage is a prime feature of the New Zealand Privacy Act. Its seamless application to both public and private sectors means that most privacy issues are able to be reached by the Privacy Act. It also means that the legislation is little affected by demarcation disputes which accompany more narrowly based laws.
- 1.4.9 The definition of “agency” includes “any person whether in the public sector or in the private sector”. In theory, therefore, even a private individual who holds information about another person is subject to the Act. However, regard must also be had to section 56 which provides that the information privacy principles do not apply to the collection of, or holding by an individual of, personal information “solely or principally for the purposes of, or in connection with, that individual’s personal, family, or household affairs”.
- 1.4.10 As far as I am aware the definition of “agency” has caused few problems of interpretation in practice. Therefore, reviewing that provision is mainly directed towards considering whether the coverage of the Privacy Act should be narrowed (by creating new exceptions) or broadened (by narrowing or eliminating existing exceptions).¹⁰ In approaching this task I have been mindful of several considerations:
- broadening the exceptions will limit privacy rights and privacy protections whereas narrowing the exceptions may provide new rights for individuals in certain circumstances;
 - creating new exceptions would relieve some agencies of existing controls but such exceptions may create anomalies in the general “seamless” application of the Privacy Act and thereby increase complexity;
 - coverage of the Act was the subject of extensive public submission to, and intense scrutiny by, the original select committee.
- 1.4.11 Therefore, I have been persuaded against creating new exceptions which would limit individual rights and erode the Act’s coverage. On the other hand, I have not lightly recommended the elimination of some existing exceptions which were the subject of careful Parliamentary scrutiny. I have done this only in cases where experience, or further reflection, suggests they are no longer needed or are unnecessarily wide.
- 1.4.12 Bodies excepted from the definition of “agency” are placed completely outside the application of the privacy principles. It would be possible to avoid this by providing *partial* exemptions. Present examples include the exemption of courts in their “judicial functions” and, in section 57, intelligence organisations remain “agencies” but have a special exemption from certain principles. I see these partial exemptions as more satisfactory than total exemption.

¹⁰ See also the discussion of exemptions at paragraphs 6.10 - 6.13.

“The National Library has not had any major difficulties in working within the framework established by the Act. The experience of the last four years has been that a common-sense approach to working through the implications of the information privacy principles has proved a successful approach.”

- NATIONAL LIBRARY,
SUBMISSION S44

- Subparagraphs (b)(i) and (ii): Sovereign, Governor-General etc*
- 1.4.13 No issues have arisen, or been raised in consultation, in relation to the exceptions directed towards the Sovereign, the Governor-General and the Administrator of the Government.
- Subparagraph (b)(iii): House of Representatives*
- 1.4.14 No submissions were made to limit or remove this exception. However, I am aware that commentators have suggested that the Official Information Act 1982 should be reformed to grant rights of access in relation to the legislative branch of government.¹¹ The matter has also been the subject of study in Canada.¹² Proponents of such a change claim that it is an anomaly in relation to notions of “open government” that rights of access to information such as advisers’ reports do not exist in relation to, say, select committees.¹³ Although the Official Information Act would benefit from its own review it is unnecessary to directly enter into that debate here.
- 1.4.15 It may be timely to consider whether personal access rights under principle 6 (or indeed other aspects of the principles) should apply to the House of Representatives. Although the access rights in neither the Privacy Act nor the Official Information Act apply to the House of Representatives this does *not* mean that an individual will never be able to obtain personal information held about him or her by the House. There are already some procedural rules in Parliamentary Standing Orders and it may be that these are adequate to stand in the place of statutory rights.
- 1.4.16 Probably the main set of personal information at issue would be submissions and evidence to select committees. The general position is that written submissions remain confidential until, at the latest, they are publicly presented to the select committee at which time they become available.¹⁴ Evidence is almost invariably given in open hearing although it is possible to give private or secret evidence in closed session.¹⁵ Private evidence will be publicly available when a committee reports but secret evidence is only released by order of the House.¹⁶ Select committee reports themselves are published. However, prior to that time draft reports, and departmental advice to committees, are generally held confidentially within the select committee system although they must be shown to people who may be adversely affected by a finding.¹⁷
- 1.4.17 Individuals are free to obtain published select committee reports and to request copies of submissions and evidence where the committee has already reported. This will usually be made available unless classified as secret. However, there are a number of provisions in Parliamentary Standing Orders which provide for allegations concerning individuals to be put to those individuals, and for information to be released on request to a person whose reputation may be damaged.¹⁸ A witness is also given reasonable access to any information that the witness has produced to a committee.¹⁹

¹¹ Grant Liddell, “The Official Information Act 1982 and the Legislature” in Legal Research Foundation, *The Official Information Act*, 1997, pages 6-18.

¹² House of Commons, *Open and Shut: Enhancing the Right to Know and the Right to Privacy*, 1997, 8-9. The Standing Committee on Justice and Solicitor General recommended that the Access to Information Act, and the Privacy Act, cover both the Senate and House of Commons.

¹³ Although there is no such *right* of access, select committees are empowered to release information to assist in consideration of a matter. See *Standing Orders of the House of Representatives*, September 1996, Standing Order 241(2).

¹⁴ Standing Order 227.

¹⁵ See Standing Orders 219 to 223. Privacy or secrecy can only be accorded to evidence with *unanimous* consent of all members of the committee.

¹⁶ Standing Order 223(3).

¹⁷ Standing Order 245.

¹⁸ See Standing Orders 226 and 239.

¹⁹ Standing Order 238.

- 1.4.18 It is pleasing to note that provisions of the type described do exist in Standing Orders to allow some individuals to obtain access to information held about them. However, the key provision, Standing Order 239, is premised upon individuals being given access to information only where their “reputation may be seriously damaged by proceedings of a select committee”. This is based upon notions of defamation or natural justice rather than individual privacy. For example, an individual could not obtain, pursuant to Standing Order 239, access to evidence given in a Parliamentary inquiry that he or she was part of a group subject to a government scientific or medical experiment.
- 1.4.19 A principal difficulty with applying principle 6 and the right of access to Parliament relates to devising appropriate complaints or review mechanisms. In particular, it may seem constitutionally inappropriate to have the actions of Parliament reviewed by an external body since this could be seen to impinge on Parliamentary privilege and the notion of Parliamentary supremacy. It may be seen as objectionable in principle for legislation to refer to internal proceedings of Parliament as this may make them inherently justiciable.
- 1.4.20 I suggest if any of the information privacy principles were to be applied to the House of Representatives that the appropriate rule making vehicle might be Standing Orders, rather than statute. The appropriate review or complaints body would be the Speaker as the final interpreter of the House’s rules (subject to the House itself). If this matter is to be taken forward, it would be best for the initiative to come from Parliament itself and I do not propose any amendment to the Privacy Act.



RECOMMENDATION 5

An appropriate committee of Parliament should consider whether it is desirable to grant individuals access rights to information held about them by the House of Representatives or to adopt rules similar to any of the 12 information privacy principles.

- 1.4.21 It is worth noting that other rules and practices of the House of Representatives do exist to protect privacy. For instance the House has a rule that names of persons should not be used in questions unless they are strictly necessary to render the question intelligible.²⁰ Furthermore, the Speaker has endorsed a policy on access to personal information in petitions which expressly addresses the right to privacy of signatories to petitions²¹
- Subparagraph (b)(iv): Members of Parliament*
- 1.4.22 The exclusion of members of Parliament in their official capacities means that a complaint against an MP that personal information had been improperly obtained, used or disclosed publicly, could not be upheld if done in an official capacity. Generally I would not investigate such allegations.
- 1.4.23 In the context of the preceding discussion concerning the House of Representatives, I have emphasised the importance of the rights of access to information. In the context of MPs, the discussion in the last few years has tended to revolve around the justification for MPs bringing personal details of individuals into the public arena. Much of the debate has centred upon the exclusion of a citizen’s rights to sue an MP for *defamation* when Parliamentary privilege can be claimed. However, for most people the right to sue for defamation is an unlikely remedy due to the costs of litigation. Furthermore, it would provide no protection for the disclosure of truthful information which nonetheless ought to have remained private.

²⁰ Standing Order 371(1)(a).

²¹ Clerk’s Office Policy, “Access to Petitions”, endorsed by the Speaker on 22 June 1988.

- 1.4.24 While Parliamentary privilege is a necessary protection for MPs acting in the public interest to expose matters, often as a last resort on behalf of citizens, it is easy for other innocent individuals to have their personal details disclosed together with those of alleged wrongdoers. Furthermore, the exclusion of “a member of Parliament in his or her official capacity” is a much wider exclusion than the exemption that would apply as an incidence of Parliamentary privilege. It follows that it might therefore be possible to narrow the exemption while still absolutely preserving the aspects of the role of an MP pertaining to proceedings in Parliament.
- 1.4.25 It has been suggested to me that there are three capacities that may need to be considered:
- *Proceedings in Parliament* - this is the core area of Parliamentary Privilege. It includes speeches in the House and at select committees and a limited amount of administrative business closely connected with proceedings of the House - for example, lodging petitions, questions and bills. It would be inappropriate to have any legislative intrusion into this area (although Standing Orders could address such issues as was discussed above in relation to the House of Representatives itself).²²
 - *The capacity of a member* - this includes proceedings in Parliament but a great deal more besides. Members’ constituency work is not normally protected by Parliamentary privilege but it is work carried out in the capacity of a member of Parliament. Also included in this category are the caucus activities of members.
 - *Outside the capacity of a member* - this includes purely personal activities, of course, but it can include official activities undertaken in a capacity other than that of a member of Parliament. One obvious example of this is activities undertaken as a Minister where the Privacy Act already clearly applies. Some Ministerial work will be transacted in Parliament and so will form part of a proceedings in Parliament, but most does not so it is outside the capacity of a member. The issue was discussed in a recent report of the Privileges Committee.²³
- 1.4.26 When the opportunity has arisen, I have encouraged Parliament to adopt procedures which can adequately protect the personal information which comes into their possession. In my report on David Caygill’s Parliamentary Privilege Bill I offered support for the proposed “right of reply” whereby individuals could answer allegations made about them and have that answer placed in Hansard.²⁴ I am pleased to note that in 1996 the new Parliamentary Standing Orders introduced a procedure for any person (other than an MP) who has been referred to in Parliament in such a way as to be readily identifiable to apply to the Speaker for a response to be incorporated into the Parliamentary record.²⁵ This is akin to the proposed right of reply.
- 1.4.27 It seems to me that a few constitutional issues would arise in applying certain of the information privacy principles to MPs. I appreciate that the most vexed areas would be in relation to principle 11 governing disclosure. However, there would probably be few problems in, for example, applying information privacy principle 5 which would oblige MPs to take reasonable security safeguards in relation to their holdings of personal information. I believe that the Parliamentary Service Commission already offers some advice to MPs in relation to security of electorate officers, for example. Nor does it seem unreasonable that

²² See paragraphs 1.4.14 - 1.4.21.

²³ Report of the Privileges Committee (into a matter concerning Mr Rodney Hide MP), May 1998, I.15C, pages 7-9.

²⁴ See report of the Privacy Commissioner to the Minister of Justice on the Parliamentary Privilege Bill, 10 February 1995. The bill was carried over into a subsequent session of Parliament and remains there, now in the name of Jonathan Hunt MP.

²⁵ Standing Orders 164-167.

where MPs collect personal information from individuals that they make them aware of the sort of matters anticipated by principle 3. I also imagine that few MPs would have any problem with the notion that they be constrained from collecting personal information by unlawful or unfair means, as provided by principle 4.

- 1.4.28 One particular issue that I would like to see some movement on is the basis upon which personal information in an MP's constituency files, or client files, are held when an MP loses office. Constituents would not necessarily wish to see their files used as political ammunition nor simply see a complete halt to any ongoing dealings on their behalf with departments or Ministers.



RECOMMENDATION 6

An appropriate committee of Parliament should consider whether it is desirable to:

- (a) adopt any measures to encourage members of Parliament to apply, or follow, any of the 12 information privacy principle; or**
(b) provide that MPs in their official capacities are agencies for some purposes of the information privacy principles.

Subparagraphs (b)(v) and (vi): Parliamentary Service Commission and Parliamentary Service

- 1.4.29 The Parliamentary Service Commission is excluded from the definition of “agency” in total. The Parliamentary Service has a partial exemption but is an agency in relation to personal information held about an employee or former employee in his or her capacity as an employee.
- 1.4.30 The Parliamentary Service Commission and the Parliamentary Service are not subject to the Official Information Act. The Parliamentary Service Commission is an “organisation” for the purposes of the Ombudsmen Act but is specifically excluded from the same term in the Official Information Act.²⁶ Accordingly, the enactment of the Privacy Act constituted an advance in terms of access to information for employees. Although a small advance, I believe that it is an important one and that partial exemptions of that type are to be preferred over total exemptions wherever they can be accommodated.
- 1.4.31 The partial exemption for the Parliamentary Service means that the information privacy principles apply in respect of employee information. A significant effect of the limitation on the exemption is that employees can access personal information held by their employer. It does not appear that the principles apply to the Parliamentary Service in respect of the collection or holding of personal information about prospective employees.
- 1.4.32 I suggest that it is timely to reconsider the total exemption in (v) and the partial exemption in (vi). I have taken the position that exceptions should not continue without good reason. This differs from the approach taken in 1993 which was, by and large, to continue any approach taken in the official information legislation so as to avoid any inadvertent consequences.²⁷ The General Manager of the Parliamentary Service has indicated that there appear to be no compelling reasons why, in fulfilling its administrative functions, the Parliamentary Service should not be fully subject to the Act.²⁸ However, he was concerned

²⁶ See Ombudsmen Act 1975, First Schedule, Part II and Official Information Act 1982, section 2.

²⁷ The extension of access rights for employees of the Parliamentary Service is an unusual case where that conservative approach was not taken. When the Privacy of Information Bill was introduced it contained only the complete exemption for the Parliamentary Service Commission. During the examination of the Bill it became clear that the position of the Parliamentary Service needed to be clarified and the partial exemption offered a good compromise between total exemption, which would have denied employees any access rights, and no exemption at all.

²⁸ Letter General Manager, Parliamentary Service, to Office of the Privacy Commissioner, 14 July 1998.

that this be achieved in a way that does not impact upon the exemption for MPs in their official capacities. I incorporate that caveat in my recommendation. I have no specific suggestion for change in respect of the Parliamentary Service Commission but I recommend that the issue be further studied by officials to see if a narrowing of the exception is possible.

- 1.4.33 I note in passing that a recent review of the Australian Freedom of Information Act has recommended that Parliamentary departments should be subject to that access regime.²⁹ In New Zealand the Office of the Clerk, which I understand to be equivalent to an Australian Parliamentary department, is already subject to the Privacy Act.³⁰ The British Columbia Information and Privacy Commissioner has recently recommended that his province's information and privacy law should be extended to the administrative operation of the Legislative Assembly, including the Offices of the Speaker, the Clerk, the Legislative Comptroller, the Sergeant-at-Arms, Hansard and the Legislative Library.³¹



RECOMMENDATION 7

Consideration should be given to whether it is appropriate to replace the total exemption for the Parliamentary Service Commission in subparagraph (b)(v) of the definition of “agency” with a partial exemption.



RECOMMENDATION 8

The partial exemption for the Parliamentary Service in subparagraph (b)(vi) of the definition of “agency” should be repealed, or further restricted, if this can be achieved in a manner that does not impact upon the exemption in subparagraph (b)(iv).

Paragraph (b)(vii): Courts

- 1.4.34 Courts and tribunals were treated differently in the Privacy of Information Bill as introduced. Tribunals were excluded in relation to their judicial functions. Courts were excluded totally. The distinction was apparently carried forward from the Official Information Act and officials were unable to find a reason for it. The Select Committee removed the distinction and both courts and tribunals are excluded in relation to their judicial functions.
- 1.4.35 Most privacy, data protection or access laws carry an exclusion of some type in relation to the courts. For example, in a recent review of the Australian Freedom of Information Act the Law Reform Commission and Administrative Review Council concluded that it would continue to be appropriate that judicial documents be excluded from that Act.³² However, I am aware of one review which has recommended that courts should be subject to a Privacy Act notwithstanding that it would be inappropriate to apply an Act such as the Official Information Act. A Standing Committee of the House of Commons of Canada recommended that the Privacy Act cover the Supreme Court of Canada, the Federal Court of Canada and the Tax Court of Canada. It stated:

“The Committee believes that the Privacy Act should extend to all federal courts and administrative tribunals, since officers and employees of such institutions should enjoy the same rights to protect their privacy as are enjoyed by

²⁹ Australian Law Reform Commission and Administrative Review Council, *Open Government: A Review of the Federal Freedom of Information Act 1982, 1995*, recommendation 73.

³⁰ There is no exception applicable to the Office of the Clerk. Furthermore, it is expressly included in the definition of “organisation”.

³¹ Information and Privacy Commissioner, submission to the Four Year Review of the Freedom of Information and Protection of Privacy Act, February 1998, page 10.

³² Australian Law Reform Commission and Administrative Review Council, *Open Government: A Review of the Federal Freedom of Information Act 1982, 1995*, paragraph 117.

other federal officers and employees. However, the Committee agrees with the approach taken in most other jurisdictions and would not extend the Access to Information Act to cover the judicial branch of Government. Accordingly, the Federal Court, the Supreme Court of Canada and the Tax Court of Canada should continue to be excluded from the ambit of the Access to Information Act.”³³

- 1.4.36 The Canadian Committee referred expressly to the position of employees and their privacy. In New Zealand, the equivalent employees are employed by the Department for Courts and their personal information is therefore already protected and they have full rights of access and correction. To the extent that the judges might somehow become involved in employment matters, or hold, use or disclose information about their employees, they would probably fall outside the definition of a court acting “in relation to its judicial functions” and therefore would probably not be an “agency”.
- 1.4.37 Undoubtedly there are numerous personal sensitivities and privacy issues in relation to matters involving the courts. Courts obtain, often through legal compulsion, various personal information, much of it of some sensitivity. As an essential feature of our judicial processes evidence is given in open court and may be publicly reported. However, it is not clear that applying the information privacy principles to judicial processes would be of very much assistance in addressing privacy issues since there is also a well developed framework, directed towards regulating the issues and respecting the competing interests.
- 1.4.38 Traditionally the courts regulated their own procedures on such issues as the manner in which personal information (evidence) is obtained and produced before the court, how the accuracy of that information is verified, and the use to which the information may be put. Over the years the legislature has become more actively involved in the processes sometimes as a reaction to privacy concerns. One need only consider the issues of giving evidence in open court and its reporting. The common law position held that justice must be seen to be done and there were virtually no exceptions.³⁴ Parliament on the other hand has actively legislated to establish courts that generally hold private hearings (the Youth Court and the Family Court), to restrict the publication of evidence given in open court, to allow the public to be excluded from courts in a range of situations, for child witnesses and others to give their evidence in a manner that they cannot be seen by the accused and, recently, for secret witnesses to give evidence without being identified.
- 1.4.39 While I do not recommend change to the partial exemption, I do express the hope that the courts (and lawyers who appear before them) recognise that their processes have the potential to significantly intrude on privacy. Very frequently this is entirely appropriate and in the public interest. However, it may be acknowledged that courts have not always been alive to the sensitivities or the effect that their own rules of procedure can have. It may be argued that a failing on the part of the courts in a previous generation has led to Parliament to establish procedures to protect sensitivities surrounding divorce, rape, child abuse and the fears for the personal safety of witnesses. I do not recommend the existing partial exemption be altered.

Subparagraph (b)(viii): Tribunals

- 1.4.40 A submission was made on behalf of a body described as the “Tribunal of the

³³ Report of the Standing Committee on Justice and Solicitor General on the Review of the Access to Information Act and the Privacy Act, *Open and Shut: Enhancing the Right to Know and the Right to Privacy*, 1987, pages 8-9.

³⁴ The common law developed a very limited exception allowing for a closed court where justice could not otherwise be done, notably in blackmail cases.

Catholic Church for New Zealand”.³⁵ As the submission makes clear, this arose out of an actual complaint made to my office.³⁶ In that case, the agency claimed that it was a “tribunal” and therefore able to take the benefit of the exception. I formed the opinion that it was not and that the exception related to tribunals forming part of the New Zealand judicial system, that is statutory tribunals.

- 1.4.41 I am unpersuaded by the submission that the definition should be altered to apply to “private” tribunals. I do not believe that it was the original intention to exempt such bodies from the Act’s requirements. Nor do I think there is a case to change the substantive position. Private bodies are not subject to the same public scrutiny and accountability as statutory tribunals which help serve to ensure rights are protected. If any change were warranted it would be to put beyond doubt that the reference to “tribunal” means a statutory tribunal forming part of the New Zealand administrative or judicial structure.



RECOMMENDATION 9

Consideration should be given to including a definition of “tribunal” limited to statutory tribunals forming part of the New Zealand administrative or judicial structure.

- 1.4.42 Alternatively, my recommendation to allow proceedings on jurisdictional issues to be taken to the Complaints Review Tribunal will enable some of the borderline issues about whether a body is an “agency” to be determined quickly and authoritatively. Another case concerning the question of whether an agency is a “tribunal” has already arisen.³⁷

Subparagraph (b)(ix): Ombudsmen

- 1.4.43 Currently the Ombudsmen are excepted from the definition of “agency”. I am not satisfied that a complete exemption is necessary or desirable. There would seem to be three features of the Ombudsmen which might at first seem to warrant an exception. These are that:
- the Ombudsmen’s status as the review authority for complaints under the official information legislation puts them in a unique position making application of the principles inappropriate;
 - as Officers of Parliament, the Ombudsmen are in a similar position to the Parliamentary bodies exempted under subparagraphs (b)(iii) - (vi);
 - as a complaints body it would be undesirable for the Ombudsmen to be subject to complaints investigation by the Privacy Commissioner.
- 1.4.44 In my view, these do not support the exemption currently bestowed. It is not clear to me that the Ombudsmen’s responsibilities as the review authority for official information complaints require them to be exempted from the information privacy principles. At most this factor would support a partial exemption covering aspects of principle 6. However, I believe that the only important issue in this context is already met by section 55(d) of the Act excluding the application of principles 6 and 7 from correspondence to or from the Ombudsmen created in the course of an investigation under the Ombudsmen Act, Official Information Act or Local Government Official Information and Meetings Act.
- 1.4.45 I do not believe that the status as an Officer of Parliament should place the Ombudsmen outside the constraints applicable to other agencies subject to the information privacy principles. Certainly no exemption is provided to the

³⁵ Submission G7.

³⁶ The point at issue in the complaint was whether the individual concerned was entitled to have a *copy* of a document. The agency was willing to let the individual inspect the document but would not, as the Act requires, make the information available in the form requested by the individual through the production of a copy.

³⁷ See *Laing v Complaints Assessment Committee*, Complaints Review Tribunal, 5 June 1998, CRT decision No. 9/98.

Auditor-General or the Commissioner for the Environment. A learned commentator on Official Information Act matters has recently questioned the inconsistent exemption of officers of Parliament from access laws and advocated reform.³⁸

- 1.4.46 It seems inappropriate that those who deal with, or are employed by, the Ombudsmen have rights under the Human Rights Act but are arbitrarily denied rights under the Privacy Act. The privacy principles should apply for instance to security breaches and to unwarranted disclosures in the course of operations. It is anomalous that an employee of that office cannot have any independent review of the result of a personal access request even though that is quite properly granted in the employment contract.
- 1.4.47 There remains the point about an Ombudsman being subject to investigation on a complaint to the Privacy Commissioner. However, this does not in itself seem inappropriate. The Privacy Commissioner can, for example, be the subject of complaint to the Ombudsmen or the Human Rights Commission. The Race Relations Conciliator and the Human Rights Commission, amongst other complaints bodies, may be subject to investigation by the Privacy Commissioner and the Ombudsmen. Some overseas privacy laws expressly apply to ombudsmen.³⁹
- 1.4.48 As the Ombudsman model itself demonstrates so dramatically, the fact that an institution is subject to a complaints mechanism does not undermine public confidence in it but rather strengthens it. I have concluded that it would be desirable for the Ombudsmen to be subject to the information privacy principles.



RECOMMENDATION 10

Subparagraph (b)(ix) of the definition of “agency” should be repealed so that the Ombudsmen are considered to be an “agency” for the purposes of the Act.

Subparagraph (b)(xiii): News media

- 1.4.49 The Privacy of Information Bill did not provide an exemption for the news media. The bill was intended to implement the OECD guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data and those guidelines did not themselves have such an exemption. Indeed, it has, until recently, been unusual for international instruments on privacy to sanction, or promote, the exemption of the news media from some form of privacy or data protection controls. Accordingly, in Europe the relevant data protection laws normally apply to the news media. Clearly there is tension between expectations of privacy and the role of free news media. This tension exists whether or not there is a privacy law or a privacy law which applies to the news media. In human rights terms this might be seen as the tension between the right to freedom of expression and to protection of privacy.
- 1.4.50 In my capacity as an adviser to the select committee studying the Privacy of Information Bill I supported the creation of an exemption for the news media. It is not a total exemption but is nonetheless fairly extensive. The exemption applies to any “news medium” (a defined term) in its “news activities” (also defined). The exemption does not extend to a news medium in its capacity as, for example, an employer or a publisher of advertising.
- 1.4.51 The press lobbied strongly against the bill and members of the select committee commented adversely that they used their editorial pages to promote their

³⁸ Grant Liddell, “The Official Information Act 1982 and the Legislature” in Legal Research Foundation, *The Official Information Act*, 1997, page 15.

³⁹ See, for example the Freedom of Information and Protection of Privacy Act, British Columbia.

commercial interests. I considered then that an exemption for the news media was appropriate because:

- there was perceived to be a significant conflict between the privacy law and the legitimate activities of the news media and the exemption would ensure that the concerns about constraints on the news media, whether or not well founded, would not eventuate;
- although some suitable rules regarding the news media ought to be developed, the information privacy principles in unmodified form were probably not suitable and would not get to the heart of many news media privacy issues;
- broadcast news media were already subject to a privacy regime in the Broadcasting Act 1989. While there was no such statutory regime for the print media, the newspapers had not exhibited the privacy invasive practices witnessed in some overseas jurisdictions.

1.4.52 Despite statements by others to the contrary, I have not changed my views but I have carefully reconsidered my position in the light of my experience, the submissions made, including from the Commonwealth Press Union, and overseas trends.

1.4.53 A complete exemption for the news media is not the only approach that can be taken to reconciling the competing human rights and public interests. For example, it might be possible to:

- provide an exemption for those parts of the news media for which adequate alternative statutory, or self-regulatory, redress is available;
- provide a partial exemption whereby, say, principles 5, 8 and 12 apply to the news media but not the others;
- give a right of access to published information about oneself but not to unpublished information;⁴⁰
- apply the principles to the news media but consider whether any of them would need exceptions written into them to meet legitimate concerns;
- apply the principles in unmodified form and if problems eventuated to provide one off exemptions under section 54 or develop a code of practice under section 46;
- provide that the principles do not apply to the news media unless, and until, a code of practice is issued;
- apply a different set of principles to the news media.

1.4.54 I think that several of these options may be feasible. The only option I would wish to completely rule out is to apply the principles in unmodified form to the news media - I have no desire to see inappropriate constraints being placed on the news media. On the other hand, I do not favour any legislative move unless it is considered all prospects of satisfactory self-regulation have been exhausted.

1.4.55 Fourteen submissions were received in relation to the exemption for the news media. Seven considered that the exemption should be reconsidered⁴¹ while 7 thought it should be left alone.⁴²

1.4.56 Interestingly, the Europeans have now moved closer to the New Zealand situation with the European Directive on Data Protection anticipating the creation of new partial exemptions from data protection laws throughout all EU countries.⁴³ One issue that I have observed since 1993 has been the practice of

⁴⁰ Some newspapers already offer Internet search facilities which make some material readily retrievable. These could perhaps be linked to a correction statement facility as well.

⁴¹ Submissions G4, G6, G12, G15, G21, G22 and S2.

⁴² Submissions G10, G11, G17, G18, S18, S42 and S54.

⁴³ See EU Directive on Data Protection, articles 29 and 30(3). See also the Working Party on the Protection of Individuals with regard to the Processing of Personal Data, Recommendation 1/97 (Data protection law and the media), February 1997.

certain magazines to publish private details about individuals. Presently magazines have taken no action to establish any sort of self-regulation notwithstanding that many of them are published by companies which also publish newspapers subject to self-regulation through the Press Council. It was suggested to me in a consultation meeting that there may be a case to limit the exemption for the news media to those organisations which are subject to:

- a statutory process by which privacy complaints can be resolved - this would cover the broadcast media;
- agencies subject to a self-regulatory regime whereby privacy complaints could be addressed - those newspapers which participate in the Press Council scheme.

1.4.57 If the exemption were to be modified in this way thought would need to be given to judging the adequacy of alternative processes. Considerable work has been done in the EU to identify what might amount to an “adequate” self-regulatory regime for the protection of privacy.⁴⁴ The two main criteria are:

- the existence of an adequate set of rules or privacy standards by which agencies bind themselves;
- the existence of procedural/enforcement mechanisms which deliver:
 - a good level of compliance;
 - support and help to affected individuals;
 - appropriate redress.

1.4.58 The Broadcasting Act’s provisions would likely meet such requirements. A set of rules is promulgated through a code of practice under the Act and individuals may complain through the statutory processes and obtain compensation (albeit that the \$5,000 limit might be subject to criticism).

1.4.59 I doubt that the Press Council would presently meet the adequacy tests expected by the EU if these standards were ever to be applied. In my view, the Press Council would provide a suitable vehicle for adequate self-regulatory protection of privacy amongst the news media if it were to:

- adopt a code setting out the standards expected of the news media concerning respect for privacy; and
- provide for compensation or redress in cases where the code has been found to be breached and the individual has suffered as a result.

1.4.60 On the first point, the code of practice ratified by the UK Press Complaints Commission on 26 November 1997 would seem to provide a good basis upon which to model a New Zealand code.⁴⁵ In respect of compensation, the \$5,000 figure provided for in the Broadcasting Act would probably cover many such complaints. A mechanism for determining compensation could readily be devised and might involve, for example, the Press Council maintaining a panel of assessors from which the successful complainant could choose to have the matter referred.

1.4.61 I do not recommend any legislative change in respect of the current exclusion of the news media in their news activities from the definition of “agency” in section 2. However, there are important privacy issues and risks in relation to news media activities and I favour industry self-regulation with provision for remedies for affected individuals. In my opinion, an Industry Ombudsman scheme may work best at a low level and enable the Press Council to deal with unresolved complaints. It may have to see witnesses sometimes to determine

⁴⁴ See, for instance, Working Group on the Protection of Individuals with regard to the processing of Personal Data, “First Orientations on Transfers of Personal Information to Third Countries - Possible Ways forward in Assessing Adequacy”, June 1997 and European Commission DGXV, “Judging Industry Self-regulation: When does it make a Meaningful Contribution to the Level of Data Protection in a Third Country?”, January 1998.

⁴⁵ Press Complaints Commission, Code of Practice, 26 November 1997.

“I look forward to the Privacy Commissioner actually producing some good work because the forces of evil will mount against it. Once the Government has those principles in place it will realise that it has not yet heard anything from Wilson & Horton Ltd.”

- RT HON DAVID LANGE, THIRD
READING OF THE PRIVACY
COMMISSIONER BILL, 10 DECEMBER
1991

credibility. Alternatively, it could receive a report from an experienced journalist who would report to the Council. I am not of the opinion that the information privacy principles would work well for the news media and if privacy needs to be protected and no adequate self-regulatory code is developed with remedies for affected individuals, separate legislation would be more satisfactory than applying the Privacy Act to the issue.

- 1.4.62 The stridency of the reaction of the press to any criticism of their self regulation, their pathological opposition to privacy laws, unmatched by any other industry, their high error rate on reporting privacy issues and the personal attacks on my office will doubtless continue in their editorial columns. Editors feel vulnerable to laws which they see as making newsgathering more expensive as their own budgets are cut. Their pleas for a more active and systematic information authority for freedom of information have a sound basis for consideration. However their proprietors have been until now steadfast about the impossibility of drafting a code of practice or providing any recompense for breaches of their own standards - even with financial caps. My only interest is in respect of complaints about privacy and there is clearly a case for attempting standards such as the British Press Complaints Commission have demonstrated can be done or principles such as the Broadcasting Standards Authority has developed over the years. A recent indication of interest in establishing some standards on privacy by the new Chairman of the NZ Press Council is, in this respect, heartening.

Collect

- 1.4.63 The term “collect” is in common usage and easily understood. However, the Act delimits its meaning by stating that it “does not include receipt of unsolicited information.” The term is not generally defined in overseas privacy laws although some use and define the related terms of “solicit” or “obtain”.⁴⁶
- 1.4.64 Two submissions suggested that the definition of “collect” be amended. Submission G12 suggested that there can be confusion as to whether unsolicited information is covered by the Act. I take the view that the position is sufficiently plain - unsolicited information is not “collected” and therefore, principles 1 to 4 do not apply, but such information is “obtained” and therefore principles 5 to 12 will apply while the information is held by an agency.
- 1.4.65 Submission G8 suggested that the definition of “collect” should include the “generation of personal information by electronic or other means”. Although I do not discount the possibility that internally generated information may be “collected” in some circumstances, I expect that in most cases such information would be considered to be “obtained” but not “collected”. In any case, it does not seem likely that collection principles would have much relevance to the processes of internally generated information.
- 1.4.66 I am not otherwise aware of any significant difficulties with the term and do not recommend any change at this time.

Correct

- 1.4.67 The correction rights in principle 7 are derived from the Official Information Act but interestingly that Act has no definition of “correct”. As the Australian Privacy Act does not define the term either it appears that the definition was created especially for the Privacy of Information Bill as a derivation of the Australian principle 7. The definition makes it clear that “correct”, in relation to personal information, means to alter information by way of “correction, deletion, or addition”. In other words, correction does not solely take its ordinary meaning but includes, if there had otherwise been any doubt, the alteration of information by way of deletion or addition.

⁴⁶ See for instance, Privacy Act 1988 (Australia) and Data Protection Bill [HL] (UK).

- 1.4.68 It is correction by way of “deletion” which raises the most issues. In particular it raises the possibility of the use of the “correction” rights in principle 7 for the purposes of seeking deletion of information which may be objectionable to an individual not so much because of any inaccuracy but because it has been obtained without the individual’s consent. Typically the issue manifests itself in requests for deletion from mailing lists. This raises issues beyond the normal sphere of principle 7 but deletion in such circumstances is seen as a practical means of remedying breaches of principle 2, 3, 10 and 11. It also draws one into a debate, which I will not canvass in this context, as to whether it is appropriate to deal with marketing list issues on an “opt in” or “opt out” basis.
- 1.4.69 The correction right in principle 7 is derived from the “individual participation principle” in the OECD Guidelines. However, that does not actually use the term “correction” but instead states:

“An individual should have the right to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.”⁴⁷

- 1.4.70 Accordingly, the OECD equivalent to the New Zealand Act’s phrase “correct, delete or add” is “erase, rectify, complete or amend.” The European Union Directive introduces a new concept in its phrase “rectification, erasure or blocking”.⁴⁸ I discuss these issues further, in the context of principle 7 itself at paragraphs 2.9.8 - 2.9.15.⁴⁹ However, I simply observe at this point the relevance of the definition of “correction” to the issue.

Document

- 1.4.71 Submission G1 suggested that in defining “document” the Act should not be so specific in naming any particular technology. It pointed out that the definition refers, for instance, to “any tape-recorder” whereas these days a tape-recorder is only one device capable of recording voice. Sound and voice is frequently recorded digitally onto computers. I certainly agree that the definition needs to remain “technology neutral” so that in the future as new technologies emerge, and existing technologies converge, the definitions remain suitable.
- 1.4.72 The definition in the Act remains surprisingly appropriate given that its lineage traces back to 1980. It has withstood the ravages of technological change remarkably well. The definition of “document” is taken from the Official Information Act 1982 but in fact its roots go deeper than that. The Danks Committee recommended the present definition. In doing so it commented:

“This definition, which is the same as that in section 48G of the Evidence Act 1908 (as inserted by section 2 of the Evidence Amendment Act 1980) and in section 1A of the Commissions of Inquiry Act 1908 (as inserted by section 2 of the Commissions of Inquiry Amendment Act 1980), is intended to be as comprehensive as possible. Comparable definitions appear in clause 4 of the Australian Bill and in clause 3 of the Canadian Bill.”⁵⁰

- 1.4.73 I consider that it would be undesirable to unilaterally change the definition of “document” while a similar definition exists in several statutes. Although the definition of document remains sound I believe that a case can be made to

⁴⁷ OECD Guidelines, clause 13(d).

⁴⁸ European Union Directive on Data Protection, article 12(b).

⁴⁹ See also recommendation 25.

⁵⁰ Committee on Official Information, *Towards Open Government: Supplementary Report*, 1981, page 61. The “Australian Bill” and “Canadian Bill” have since been enacted.

redefine it to either simplify its elements (by *removing* the examples of particular technology such as tape-recorders) or to make its illustrative value more relevant (by *adding* examples of modern technology, such as CD-Roms which did not exist in 1980). If change is made, it is desirable that this be done in conjunction with amendment to the definition of “document” in the official information and evidence statutes. It is therefore timely to note that the Law Commission has, in the course of its evidence law review, proposed the following new definition of “document”:

“**Document** means any record of information and includes:
 (a) anything on which there is writing or any image; and
 (b) anything on which there are marks, figures, symbols or perforations having a meaning for persons qualified to interpret them; and
 (c) anything from which sounds, images or writing can be reproduced, with or without the aid of anything else.”⁵¹



RECOMMENDATION 11

Consideration should be given to adopting a new definition of “document” in section 2 in conjunction with any redefinition of the term in the proposed Evidence Code.

Individual

1.4.74 The information privacy principles apply solely in relation to any “individual” as defined, that is “a natural person, other than a deceased natural person.” Although some submissions were made that it would be possible to state the definition more plainly⁵² or that it would be useful to define “natural person”⁵³ I consider that the definition is satisfactory. Clearly an “individual” is a living person - not a dead person.

1.4.75 However, the matter is complicated by the fact that section 46(6) redefines the term “individual” in relation to codes of practice concerning “health information”, as defined in section 46(7). The issues arising from this are discussed below in relation to section 46 at paragraphs 6.2.17 - 6.2.21.⁵⁴ If the recommendations to amend sections 46(6) and (7) are adopted, Parliamentary Counsel should consider whether there needs to be an amendment to “individual” in section 2 as well. Otherwise if more extensive use is made of section notes in future, it may be useful to provide a cross reference between the two definitions.

Information privacy principle

1.4.76 The definition of “information privacy principle” is quite plain and does not, in my view, require change. However, I record that, for a full understanding of how the Act works, it is necessary to be aware that section 53 of the Act, which outlines the effect of a code of practice, means that in some instances references in sections of the Act to an “information privacy principle” need to be read as references to a rule in an applicable code of practice.

Permanent resident of New Zealand

1.4.77 The term “permanent resident of New Zealand” appears only in section 34 and therefore it may be advantageous to users of the Act to move the definition from section 2 into that section. However, I have separately recommended that the standing requirements in section 34 should be repealed or amended.⁵⁵ If

⁵¹ The Law Commission, *Draft Evidence Code*, March 1998.

⁵² Submission G1.

⁵³ Submission G12.

⁵⁴ See also recommendation 75.

⁵⁵ See recommendation 61.

the section is repealed this definition should also be repealed. If section 34 is amended, or some distinction continues to be made between citizens, permanent residents and others, there may continue to be a need for this definition.

Personal information

- 1.4.78 “Personal information” is defined consistently with the definition of “personal data” in the OECD Guidelines.⁵⁶ The definition is a derivation of one that appeared in the Official Information Act 1982. It is a term that is central to the Privacy Act’s operation and is satisfactory for that purpose.
- 1.4.79 The only complication in relation to the definition is the phrase that states that the term “includes information contained in any register of deaths that is maintained by the Registrar-General pursuant to the Births, Deaths, and Marriages Registration Act 1995, or any former Act”. This makes it clear that information about deceased persons is encompassed within the term in relation to information held on the deaths register. The main reasons for making this clear relate to the application of the:
- public register controls in Part VII of the Act; and
 - the information matching controls in Part X of the Act.⁵⁷
- 1.4.80 However, a complication arises because the definition encompasses information “contained in” the register of deaths leaving open the position of information sourced from, but no longer contained in, the register (that is, after the information has left the register and is in the hands of another person). That of itself is not problematic in relation to obligations on the Registrar of Deaths under the public register privacy principles. However, it might call into question the effectiveness of public register privacy principle 2 as it applies to *other* persons using information sourced from the deaths register. It might also lead to interpretational complications if an information matching programme were to be authorised involving the register of deaths.



RECOMMENDATION 12

Consideration should be given to amending the definition of “personal information” to clarify the position of information sourced from, but not contained in, the register of deaths.

Public register

- 1.4.81 The definition of “public register” is discussed in relation to section 58 at paragraphs 7.2.4 - 7.2.11.

Public sector agency

- 1.4.82 In reviewing the definitions I have given consideration to any opportunity to “unclutter” a key interpretation section in the Act. In some instances the interpretation provisions may be over-elaborate due to complexities inherited from other statutes. Accordingly, I have sought out opportunities to delete or combine definitions and to remove complexities.
- 1.4.83 The definition of “public sector agency” appeared to offer possibilities in that regard. Although the definition itself is not taken from the official information legislation the concept, and most of the constituent parts of the definition, are derived from the two official information statutes and the Ombudsmen Act. The current definition is perfectly workable and I have no particular wish to alter the position *in substance*. However, I consider that it may be possible to

⁵⁶ Article 1 defines personal data to mean “any information relating to an identified or identifiable individual”.

⁵⁷ The Privacy Commissioner Act 1991, and the Privacy Act 1993 at the time of its enactment, provided for information matching involving the deaths register. Although that provision was dropped at the time of the consolidation exercise involved in enacting the Births, Deaths and Marriages Registration Act 1995, it is anticipated that information matching involving the deaths register may again be authorised at some future time.

more briefly express the definition by combining and simplifying the constituent parts (by which I mean the definitions of department, local authority, Minister and organisation).

1.4.84 Accordingly, I considered the following possible definition:

Public sector agency:

(a) means an agency that is:

- i a Minister;
- ii a Government department named in Part I of the First Schedule to the Ombudsmen Act 1975;
- iii an organisation named in Part II of the First Schedule to the Ombudsmen Act 1975 or the First Schedule to the Official Information Act 1982, or both;
- iv a local authority or public body named or specified in the First Schedule to the Local Government Official Information and Meetings Act 1987 including any committee or subcommittee which the local authority is empowered to appoint, and a committee of the whole authority; and

(b) includes:

- i the Office of the Clerk of the House of Representatives;
- ii an intelligence organisation; and
- iii any agency that is an unincorporated body (being a board, council, committee or other body) established in accordance with the provisions of any enactment or by any such public sector agency for the purpose of assisting or advising, or performing functions connected with, any public sector agency within the meaning of paragraph (a) or (b).

1.4.85 If this definition is adopted then it may be possible also to repeal some, or all, of the definitions of department, organisation, and local authority. The need for some of those other definitions is, in any case, diminished by some of the other recommendations I make.⁵⁸ I suggest leaving the definition of “Minister” because that will continue to be needed notwithstanding other recommendations I am making. Where it is necessary to refer to a term which is no longer defined, it would be possible to, for example, refer to “a local authority within the meaning of paragraph (a)(iv) of the definition of public sector agency”.

1.4.86 However, if my recommendation to amend the definition of “public sector agency”, and to repeal the constituent definitions, is not accepted I nonetheless suggest that consideration be given to simplifying aspects of these five definitions and the clause I have tentatively set out above may suggest a way to do this.⁵⁹



RECOMMENDATION 13

Consideration should be given to redefining or recasting “public sector agency”, “Minister”, “department”, “organisation” and “local authority”.

1.4.87 Consideration should also be given to defining as a class those agencies that are not public sector agencies. The obvious title would be “private sector agency”. A suitable definition might be:

Private sector agency means an agency which is not a public sector agency.

⁵⁸ Such as recommendations 34, 70, 115 and 147.

⁵⁹ For example, “local authority” could be defined somewhat more simply than at present through the formulation set out at paragraph (a)(iv) of the proposed definition of public sector agency.

- 1.4.88 The usefulness of this term lies in the fact that it could be used to replace various references in the Act to “any agency that is not a public sector agency”. Such references can be found in sections 3, 35 and 46. Section 35 concerning the making of charges will particularly benefit from the resultant simplification.



RECOMMENDATION 14

Consideration should be given to enacting a definition of “private sector agency”.

Publicly available information and publicly available publication

- 1.4.89 “Publicly available information” is a term that is used in several of the exceptions to the information privacy principles.⁶⁰ The term is not as wide as might first be thought as the definition makes it clear that it means personal information that is contained in a “publicly available publication” which is defined to mean:

“a magazine, book, newspaper, or other publication that is or will be generally available to members of the public; and includes a public register”.

- 1.4.90 The definition of publicly available publication is derived from the definition of “generally available publication” in the Australian Privacy Act 1988 although that Act does not use the term as the basis of an exception in the way that the New Zealand Act does. The Australian definition of “generally available publication” is expressed to mean “a magazine, book, newspaper or other publication that is or will be generally available to members of the public”.⁶¹
- 1.4.91 The inclusion of exceptions related to publicly available information may be argued to contribute to the workability of the Privacy Act since it might be difficult to apply privacy principles to personal information in publications where there is, by definition, no control over how they are used and disclosed because of their “public availability”.
- 1.4.92 Whether something is a “publication” that “is or will be generally available to members of the public” is not always clear. The Act deems public registers to be included in the definition but there is less certainty with regard to such materials as:
- statutory registers that are not “public registers” listed in the Second Schedule;
 - official reports to which the public is entitled but which have not been published;
 - material made available on an Internet site.
- 1.4.93 I merely mention these areas of possible interpretational difficulty. I await a suitable case to form an opinion on such questions, which can, in turn, be subject to definitive interpretation by the Tribunal if necessary.
- 1.4.94 There are some other types of information which, in other contexts have been described as being “in the public domain” (this term is not used, and is generally inappropriate, in respect of information privacy legislation) such as information that has been broadcast. For instance, a tape recording made by an individual of a radio broadcast would not constitute “publicly available information” in terms of the definition (although a cassette tape on sale commercially might constitute a “publicly available publication”). Another non-traditional type of publication would be an “electronic book” supplied on a disk or CD-Rom. Where such an electronic publication is made generally available to members of the public I have little doubt that it would be considered a “pub-

⁶⁰ See information privacy principles 2(2)(a), 10(a) and 11(b).

⁶¹ Privacy Act 1988 (Australia), section 6.

licly available publication” (although the issue has yet to be tested in a complaint).

- 1.4.95 None of the examples that I have just mentioned warrant, in my view, amending the definitions. However, there is one circumstance in which I believe action is warranted since otherwise an anomaly may exist. This relates to the inclusion of “public registers” in the definition. “Public register” is defined in sections 2 and 58 essentially to mean a register, roll, list or other document maintained pursuant to a public register provision listed in the Second Schedule. In other words, only some registers, rolls etc maintained pursuant to statutory provisions are “public registers” for the purposes of the Act. Accordingly, it appears to me those other registers or rolls etc will only be “publicly available publications” if they can be characterised as falling within the first part of the definition, that is being a “magazine, book, newspaper, or other publication”. Some registers are actually maintained in books. Some others are, from time to time, published in book form.⁶² Accordingly, there exists a potential anomaly whereby information or documentation having very similar characteristics in terms of being publicly available may, depending upon certain formatting issues, perhaps fall outside the relevant definitions.
- 1.4.96 Any expansion of the definition of publicly available publication will, in effect, diminish the application of the privacy principles through the widening of the exceptions. However, that may be appropriate if one accepts the basic premise that an exception is necessary.
- 1.4.97 In recommendation 96 I have suggested that a process be undertaken to bring statutory registers open to public search into the list in the Second Schedule. As that work advances the extent, and effect, of any anomaly is diminished. That of itself is an appropriate response and that therefore it is unnecessary to broaden the definition of “publicly available publication” to include other registers maintained pursuant to law which are open to public search.

Statutory officer

- 1.4.98 The term “statutory officer” is only used in section 3 and it seems to make more sense that the definition should be placed in that section. This will ensure that people using section 3 are aware of the defined term while uncluttering section 2 for definitions of general application.



RECOMMENDATION 15

The definition of “statutory officer” should be moved from section 2(1) into section 3.

Working day

- 1.4.99 “Working day” has an importance in relation to those places in the Act where time periods are expressed. For example, section 40 makes it clear that a decision on an information privacy request is to be made as soon as reasonably practicable and in any case “not later than 20 working days” after the day on which it is received. The definition differs from that contained in the Interpretation Bill now before Parliament since it excludes the period between 25 December and 15 January.
- 1.4.100 The only context in which I can recall any problems being ascribed to the definition in section 2 is in relation to information matching under Part X, which has its own additional set of definitions in section 97. Unfortunately, on occasion people working with Part X have failed to familiarise themselves with the other Parts of the Act including the definition of “working day”. The defi-

⁶² The register of medical practitioners, for example, is not currently listed as a public register but is open to public search and, from time to time, is published as a supplement to the *New Zealand Gazette*.

inition of working day applies throughout the Act, including Part X. Agencies involved with information matching may need to make themselves more familiar with section 2 but I recommend no change to the Act in this respect.

New definitions

- 1.4.101 In submissions, suggestions were variously made as to the merits of new definitions for:
- public interest;
 - indexed or organised;
 - search reference;
 - electronic transmission;
 - statutory register;
 - disclosure;
 - use;
 - obtain;
 - reasonable;
 - research purposes.
- 1.4.102 I considered the merits of each of these suggestions and others. I have suggested elsewhere that consideration be given to defining “tribunal” and “trade secret”.⁶³ However, “use” is the only other term which I consider may warrant definition at this stage.⁶⁴

Use

- 1.4.103 An issue has arisen overseas as to whether “browsing” constitutes a “use” of information under a privacy or data protection law. An English case suggests that simply reading personal information, but not to employ that information for a purpose, may not constitute “use”.⁶⁵ In that case it could be shown that a police officer had checked a confidential police database for details of debtors being investigated by his friend but it could not be proved that the information had indeed been passed on or actually put to a use. The court treated the accessing of the computer records as a pre-requisite to use rather than use itself.
- 1.4.104 The Data Protection Bill presently before the UK Parliament defines “processing” of personal data to include “retrieval, consultation or use of the data”.⁶⁶ It would appear that if browsing of data does not constitute “use” then it will almost certainly constitute “retrieval” or “consultation”. It may be that this is the legislative response to the problem thrown up by the earlier case.
- 1.4.105 I too had to form a view on the meaning of the “use” in an information privacy principle 8 case where an agency stored and retrieved information but nothing else had apparently happened. In the circumstances of that case, I concluded that in order to show that some usage had occurred, the retrieval would need to have been followed by some action. In that case, the inaccurate information was simply deleted.⁶⁷ However, browsing is not really an issue in respect of the way “use” is used in principle 8. Browsing is essentially a problem involving authorised users of a database accessing information they have no business in seeing or using. It is therefore more of an issue in respect of principles 5 and 10 than principle 8 and the issue has not yet been tested in New Zealand under those other principles.
- 1.4.106 Browsing of sensitive personal information by employees of the Internal Revenue Service caused a scandal in the USA in 1993/94 and in subsequent years. Internal audits in 1997 confirmed a worrying level of browsing by IRS employees of confidential tax files of notable people and others.⁶⁸ As a result the IRS

⁶³ See recommendations 9 and 50.

⁶⁴ The Privacy of Information Bill did define “use” but the definition was omitted by the Select Committee. However, the original definition would not have addressed the issue discussed here.

⁶⁵ *R v Brown* [1996] 1 All ER 545.

⁶⁶ Data Protection Bill [HL] (UK), 4 June 1998 version, section 1(1), paragraph (b) of definition of “processing”.

⁶⁷ Case note 9257.

⁶⁸ Reportedly 1515 IRS workers had been investigated for browsing through tax files. See “Surprise? Browsing Tax Files still a Problem at IRS” 17/8 *Privacy Times*, 17 April 1997, page 3.

prosecuted some staff. However, the US Federal Court of Appeals held in one important case that an IRS employee could not be convicted because he merely looked at confidential tax data for unauthorised purposes but was never proven to *use* the information as part of a fraudulent scheme. A report of the case⁶⁹ suggested that the defendant was a member of a white supremacist group who regularly snooped through the IRS’s computerised integrated data retrieval system. Targets included tax returns of members of a political campaign, the tax return of an assistant district attorney (who had been prosecuting the defendant’s father on an unrelated charge) and his wife, the tax return of a city councillor’s campaign committee (who had defeated the defendant in a council election), the tax return of his brother’s instructor, and the tax return of a woman the defendant had dated a few times, amongst others. The actions, although reprehensible, could at most lead to a dismissal of the employee but not the prosecutions that the IRS had laid.

- 1.4.107 The US decision prompted an IRS Commissioner to ask Congress for legislative amendments to make such browsing a felony. As a result the Taxpayer Browsing Protection Act was enacted into law on 5 August 1997. That law makes it a misdemeanour for an IRS employee to review tax records without authorisation. The law also creates a civil remedy based on an unauthorised inspection of tax return information and requires the IRS to notify taxpayers when an IRS employee is indicted or otherwise charged for improper browsing of their information.⁷⁰
- 1.4.108 Browsing of taxpayer files by staff has also been uncovered at the Australian Tax Office. Successful prosecutions have been brought under the ‘computer crime’ provisions in the Commonwealth Crimes Act.⁷¹ There are no equivalent computer-related offences in the New Zealand Crimes Act as discussed at paragraphs 12.16.13 - 12.16.16.
- 1.4.109 It seems to me that the unauthorised retrieval or consultation of personal information in the circumstances known to have occurred in the UK, USA and Australian cases is the proper subject of the information privacy principles. Such browsing could easily be as serious as some other incidental or administrative use of information which already falls within the scope of the principles. It appears from some of the reports of browsing that the issue often concerns a matter of proof. The authorities have been able to prove that an employee consulted certain confidential records for which they had no proper purpose but could not show that the employee actually disclosed the information to someone else or used it in some way.
- 1.4.110 The matter could be taken forward in several ways. One might be to define “use” to include the elements of browsing. A suitable definition might be as follows:

“use, in relation to information, includes retrieval, consultation or use of information.

There was considerable interest in submissions in the proposal to define “use” to encompass browsing with responses, mixed, but generally favouring the issue being addressed.⁷²

⁶⁹ See “Unauthorised Access to IRS Files not a Felony, Court says”, 17/6 *Privacy Times*, 19 March 1997, 1-2. A Tennessee jury on similar grounds acquitted as IRS employee caught snooping through the records of such celebrities as Lucille Ball, Elvis Presley, Elizabeth Taylor and Tom Cruise (see *Privacy Times*, 17 April 1997).

⁷⁰ The report on the new Act is taken from “Legislative Round-up” 5/1 *Privacy & American Business*, March/April 1998, 14.

⁷¹ See “Raiser v Slodac (1995)” in 5 *Privacy Law & Policy Reporter* (1998) 13.

⁷² See submissions K11-K14, K18, K19, K21, K24, K28, K29, S13, S19 and S42.

“To extend the meaning of ‘use’ to incorporate ‘browsing’ would potentially be to penalise an action which has no recognisable consequences.”

- NZ EMPLOYERS

FEDERATION, SUBMISSION K14

- 1.4.111 An alternative would be to tackle the issue of browsing in the relevant principles. Accordingly, the issue could be tackled in, say, principle 5, but principles 8 and 10 could be left as they are. I recommend that further consideration should be given to defining the term “use” in section 2. However, my principal recommendation is to take the matter up in principle 5 and I discuss this elsewhere.⁷³



RECOMMENDATION 16

Consideration should be given to the desirability of enacting a definition of “use” which will encompass the retrieval, consultation or use of information.

Section 2(2)

- 1.4.112 Subsection (2) is an 89 word sentence provided “for the avoidance of doubt”. It has been criticised for being lengthy and convoluted. In fact, with a little study, the ideas conveyed in the provision do not seem particularly complex. However, apparent complexity is compounded by the fact that it links to a subparagraph in the definition of “agency” which is, itself, expressed in a perplexing way (a commission of inquiry, etc, “appointed, pursuant to, and not by, any provision of an Act...”).
- 1.4.113 The provision is included out of an abundance of caution. Given my desire that the statute be user-friendly for lay people, I am concerned to have such drafting in the key interpretation section. I recommend that the provision be redrafted in a plainer fashion if possible. It should be noted that part of the phraseology is also used in section 55(c) and there is a need for consistency.



RECOMMENDATION 17

Section 2(2) should be replaced with a more concise provision.

1.5 SECTION 3 - Information held by agency

- 1.5.1 Section 3 sets out the circumstances where information is deemed to be held by an agency. Information held in an official, employment, or membership capacity is deemed to be held by the agency itself, as is information held by another agency where that agency is linked by an agency or bailment relationship, or a contractor relationship limited to data processing only, and where it does not use or disclose the information for its own purposes.
- 1.5.2 I have already noted that “statutory officer” is used in this section but not elsewhere in the Act. I have therefore made the suggestion that the definition be removed into section 3 for convenience of users. “Statutory officer” is a term derived from the Official Information Act 1982 and has been interpreted in that context. It has not yet been the subject of consideration by the Complaints Review Tribunal in the context of the Privacy Act.

1.6 SECTION 4 - Actions of, and disclosure of information to, staff of agency, etc.

- 1.6.1 This section provides that for the purposes of the Act agencies are responsible for the actions of, or information disclosed to, their employees. Similarly, section 126(1) provides that for the purposes of the Act employee’s actions are to be treated as the employer’s - whether or not the latter knew or approved of them. However, in any proceedings under the Act the employer will have a defence under section 126(4) if he or she took “such steps as were reasonably practicable” to prevent the employee taking that action or actions of that type.
- 1.6.2 It is unfortunate that it is necessary for employers and employees to locate

⁷³ See recommendation 23.

“Sections 3 and 4, together with section 126 do not, in practice, appear to have caused any particular difficulty, although situated at opposite ends of the statute. There could, however, be an inherent difficulty for some smaller employers in grasping the initial fact that they are covered by the term ‘agency’. This is something which requires education rather than legislative tinkering.”

- NZ EMPLOYERS FEDERATION,
SUBMISSION G10

sections in opposite ends of the statute to obtain the complete picture. However, I believe that an employer who reads both sections will obtain a relatively plain message as to the combined effect of the provisions. I have earlier concluded that it will be undesirable to switch the order of sections or generally change the Act's existing numbering system and structure. Accordingly, while the position is not ideal I do not recommend change. However, if, at some stage, greater use is made of endnotes in statutes I suggest that a cross-reference be provided.

1.7 SECTION 5 - Act to bind the Crown

- 1.7.1 Clause 27 of the Interpretation Bill, presently before Parliament, provides that no enactment binds the Crown unless it expressly provides that the Crown is bound. That clause re-enacts section 5(k) of the Acts Interpretation Act 1924. If the Law Commission's recommendation to reverse that statutory presumption ultimately prevails it may no longer be necessary to have a provision such as section 5. However, subject to any need to reconsider the matter if the Interpretation Bill is amended, there is no reason to alter section 5.

Part II

II

Information Privacy Principles

57

“With regard to the rest of the Privacy Act 1993, our members do not report any major difficulties and have found that compliance is largely a matter of good business practice.”

- Insurance Council of New Zealand, submission L9

“We understand that a number of people have suggested that changing the expression and ordering of the information privacy principles at this point is unnecessary given their broad general acceptance in the community. We submit that the complexity, repetitiveness, and illogical ordering of some of the principles and their associated provisions are major barriers to the understanding of the Act and urge that consideration be given to a major reorganisation exercise.”

- NZ Law Society Privacy Working Group, submission K29

“A member country should refrain from restricting transborder flows of personal data between itself and another member country except where the latter does not yet substantially observe these guidelines or where re-export of such data would circumvent its domestic privacy legislation”.

- OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 1980, clause 17

2.1 INTRODUCTION

2.1.1 Part II includes 6 sections:

- *section 6*: the principles themselves;
- *section 7*: which saves the effect of certain other enactments;
- *section 8*: which sets out the application of the principles to information collected, obtained or held before or after the Act’s commencement;
- *section 9*: postponing the application of the disclosure principle to lists used for direct marketing to mid-1996;
- *section 10*: applying the principles to certain information held overseas;
- *section 11*: governing the enforceability of the principles.

2.1.2 The information privacy principles are at the heart of the Privacy Act. In other countries it is common for privacy or data protection acts to contain sets of principles. It has been found to be an appropriate means of translating the concepts of information privacy into a legally effective form.

“The Privacy Act has not been a burden for many agencies. Public complaints about compliance costs may be exaggerated. The generally non-prescriptive nature of the legislation confers advantages in comparison with overseas models.”

- NZ LAW SOCIETY PRIVACY WORKING GROUP, SUBMISSION WX12

Origins of the principles

- 2.1.3 The information privacy principles, established in accordance with the OECD’s 1980 Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (the “OECD Guidelines”), concern:
- the collection, use, and disclosure, by public and private sector agencies, of information relating to individuals; and
 - access by each individual to information relating to that individual and held by public and private sector agencies.
- 2.1.4 The OECD Guidelines contain their own set of 8 principles, known respectively, as the:
- collection limitation principle;
 - data quality principle;
 - purpose specification principle;
 - individual participation principle;
 - security safeguards principle;
 - openness principle;
 - use limitation principle;
 - accountability principle.
- 2.1.5 The information privacy principles do not directly repeat the OECD principles but are designed to suit New Zealand law and circumstances and to be somewhat more precise. They owe much to the principles in the Australian Privacy Act 1988 although there are notable differences.

Principles or sections?

- 2.1.6 Many modern privacy laws contain sets of information privacy principles, data protection principles or fair information principles. For example, amongst common law countries there are sets of principles in the laws in the UK, Ireland, Australia and Hong Kong. Principles have been proposed for laws under consideration in Victoria and New South Wales. However, not all data protection or privacy laws set out principles. The Canadians legislated to implement the OECD guidelines in a more traditional manner with the content of what are principles in our Act set out as sections in a statute.
- 2.1.7 In New Zealand, the former Information Authority devised its own set of principles concerning collection, use (including disclosure) and access (including correction).¹ Notwithstanding the usefulness of principles conceptually, and its support for privacy legislation to be based on a generally applicable set of principles, the Authority was not convinced of the merit of including the principles themselves directly in legislation. Its 1988 report stated:

“Should there be principles or rules?

It was suggested that consideration should be given to having ‘principles’ instead of ‘rules’ in the legislation that governs collection and use of personal information. The United Kingdom Data Protection Act and the proposed Australian Privacy Bill are cited as examples of this approach. However, the Canadian, USA, Quebec and Ontario legislation can be quoted as examples of a rules approach. The latter Acts are clearer for all who operate the legislation to understand - those collecting, using and supplying the information and for the complaints review body.”²

- 2.1.8 Notwithstanding the Information Authority report, the two bills brought before the New Zealand Parliament substantially dealing with the subject each set out a series of principles.³ A decisive factor may have been the enactment of the Australian Privacy Act 1988 with a set of principles. New Zealand, of course, has a

¹ Information Authority, *Personal Information and the Official Information Act: Recommendations for Reform*, 1987, page 12.

² Information Authority, *Report on the Subject of Collection and Use of Personal Information*, May 1988, AJHR E27B, paragraph 25.

closer economic relationship with Australia than the North American jurisdictions which have adopted a “rules” approach. By the time the New Zealand bill was introduced the Australian Act was successfully operating for several years.

- 2.1.9 Now that the Privacy Act has operated for five years with a set of principles it would be an unattractive proposition to rewrite the law in substantially the same fashion with a “rules” approach. Nonetheless, it is acknowledged that the use of “principles” in legislation is unusual and the novelty of the legislative approach can give rise to interpretational issues over and above the content of the principles.⁴ There has been some generalised criticism that the principles make the law too imprecise and that something more prescriptive is necessary so that lawyers can explain how the law applies to specific fact situations. My experience is that those who are working on a day to day basis with the Act do not make this complaint. They see the flexibility in the principles. Lawyers look for precedent decisions and there have been few of these. That is probably the real source of the criticism of the principles by those not familiar with how the law is working in practice.
- 2.1.10 In a sense the Information Authority’s distinction between “principles” and “rules” is not entirely valid - principles can be “rules” as effectively as other sections in a statute. Fashioning parts of the statute into principles is not necessarily more significant than, say, placing material in a schedule.⁵
- 2.1.11 I do not recommend a departure from the Act’s approach in establishing a set of principles. My primary examination in respect of the principles has been directed towards their content and coverage - is any change necessary or desirable? I also took the opportunity of consultation to canvass whether there should be any new principles.⁶

SECTION BY SECTION DISCUSSION

2.2 SECTION 6 - Information privacy principles

- 2.2.1 Section 6 sets out the 12 information privacy principles. The principles are based upon the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data and, in many respects, have been copied from the principles in the Australian Privacy Act 1988 (with some important changes). Throughout the principle by principle discussion which follows reference is made to both the OECD Guidelines and the Australian principles.
- 2.2.2 Also included in the discussion is reference to similar principles, and provisions, in comparable legislation in other jurisdictions and, in some cases, in international instruments. For the most part the thinking behind the principles can be dated to 1993 (when the select committee concluded its examination), 1991 (when the Privacy of Information Bill was finalised and introduced) or 1988 when the Australian principles were enacted.⁷ Accordingly, it has been

³ See the Hon Peter Dunne’s Information Privacy Bill and the Privacy of Information Bill. There were two much earlier bills, the 22 clause Preservation of Privacy Bill 1972 and the 18 clause Privacy Commissioner Bill 1974, but neither addressed information privacy issues in a substantive way. The 1972 bill would have required registration of computer installations with individual access rights while the 1974 bill would have done little more than establish a Commissioner.

⁴ Discussed in my address to the 1996 NZ Law Conference “Principles in Practice: Challenges for Lawyers”.

⁵ Having said that, the Act makes some distinctions between material in the principles and otherwise but this is a matter of statutory detail rather than the fact that they are labelled “principles”.

⁶ Forty-seven submissions were received on the discussion paper on the existing privacy principles with a further 27 on possible new privacy protections.

⁷ Indeed, one might even delve further and attribute some of the thinking to 1980, the date of the OECD Guidelines, which were themselves a culmination of 1970s experiences.

valuable to test the principles, and their drafting, against approaches taken in recent privacy legislation. There has been a considerable amount of recent legislation to ponder as can be seen at Appendix C.

2.2.3 In looking at other statutes, I have concentrated my attention on comparable jurisdictions. I have found material of value in the Canadian provincial legislation - particularly the British Columbia Act (upon which many of the subsequent provincial laws have been modelled). I have also had regard to the Hong Kong law since, like the New Zealand Act, it covers both the public and private sectors. I am aware that the New Zealand Act was studied by those responsible for drafting the Hong Kong law.

2.2.4 In addition to the influence of the OECD Guidelines and the Australian Act on the shape of the principles, there are several specifically New Zealand influences which I have kept in mind and have occasionally referred to in the report. Principal amongst these was the work of the Justice and Law Reform Select Committee which studied the Privacy of Information Bill. A further major influence in respect of principles 6 and 7 is the official information legislation which had as its origin the reports of the Danks Committee.

2.3 PRINCIPLE 1 - Purpose of collection of personal information

International origins and comparisons

2.3.1 Principle 1 is derived in part from the OECD collection limitation principle which provides:

“Collection limitation principle

There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means, and where appropriate, with the knowledge or consent of the data subjects.”

2.3.2 The OECD collection limitation principle is supplemented by a “purpose specification principle” and “use limitation principle” which ensure that the purposes for which information are collected are made plain and any subsequent use and disclosure is limited to such purposes. The Act, in common with the Australian Privacy Act, sets out the collection, purpose specification and use and disclosure controls in separate principles. The Council of Europe Convention No. 108 is of similar effect but combines obtaining personal data and constraint on subsequent use into a single provision often referred to as the “finality principle” (although that term is not actually used in the text of the Convention).⁸ The most recent European restatement of the concept is contained in the European Union Directive on Data Protection which states:

“Member states shall provide that personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.”⁹

2.3.3 The new UK Data Protection Bill’s equivalent to principle 1 has been prepared to meet the requirements of the EU Directive. It states:

“Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.”¹⁰

⁸ Convention No 108, article 5.

⁹ EU Directive on Data Protection, article 6(1)(b).

¹⁰ Data Protection Bill [HL], (UK), 4 June 1998 version, Schedule 1, Part I, Principle 2.

“Principle 1 has been of great educational benefit, forcing us to consider the necessity and worth of all information we collect, not just personal information.”

- FRANKLIN DISTRICT COUNCIL, SUBMISSION K8

2.3.4 The Hong Kong privacy law, which was passed after the Act, closely follows the New Zealand and Australian models but adds an additional paragraph (c). It states in full:

- “Personal data shall not be collected unless:
- (a) the data are collected for a lawful purpose directly related to a function or activity of the data user who is to use the data;
 - (b) subject to paragraph (c), the collection of the data is necessary for or directly related to that purpose; and
 - (c) the data are adequate but not excessive in relation to that purpose.”¹¹

2.3.5 The Hong Kong ordinance was largely based upon recommendations of the Law Reform Commission of Hong Kong but the additional paragraph (c) does not appear to have originated from the Commission’s report.¹² The Law Reform Commission explicitly recommended adoption of the OECD collection limitation principle. It appears that the reference to “adequate but not excessive” is an attempt to combine the language of the European instruments with that of the OECD collection principle.¹³ This may have been done to more clearly ensure “adequacy” in terms of the EU Directive which was an explicit consideration for the Hong Kong Government.¹⁴

2.3.6 The notion of collecting “adequate but not excessive” information is consistent with the OECD Guidelines even though the phrase is not used. In my view, something very similar is required by the word “necessary” in our own principle 1. If the collection of the information is “excessive in relation to the purpose” it may equally be argued that the information is not “necessary for that purpose”. Although the Hong Kong principle appears to have achieved a good synthesis between the OECD guidelines and the EU Directive on this issue I do not recommend the adoption of its paragraph (c) in our principle. While the Hong Kong approach may, on balance, be preferable to our own principle 1 I do not think that the difference would warrant change from a principle with which users of the Act have become familiar. Further, I do not believe that the absence of the words “adequate and not excessive” would concern the Europeans when judging the adequacy of the safeguards provided by our law.

2.3.7 Most submissions expressed satisfaction with principle 1.¹⁵

2.4 PRINCIPLE 2 - Source of personal information

2.4.1 Principle 2 provides that where an agency collects personal information, the agency must collect the information directly from the individual concerned. There are a variety of exceptions set out in principle 2(2).

Rationale, origins and overseas comparisons

2.4.2 The rationale for principle 2 might be explained in several ways:

- by directing agencies to collect information directly from the individual, the individual concerned is empowered to refuse participation in the infor-

¹¹ Personal Data (Privacy) Ordinance 1995 (Hong Kong), Schedule 1, principle 1(1).

¹² See Law Reform Commission of Hong Kong, *Report on the Reform of the Law relating to the Protection of Personal Data*, 1994, paragraphs 9.5 and 9.15.

¹³ The phrase “adequate, relevant and not excessive in relation to the purposes for which they are collected” is a phrase which appears in article 6(1)(c) of the EU Directive on Data Protection.

¹⁴ EU countries must place restrictions on the transfer of personal data to countries which do not provide “adequate” safeguards - see EU Directive on Data Protection, article 25 discussed at paragraph 2.18.12.

¹⁵ See submissions K8, K9, K11, K14, K18, K20-K22, K25, K27, K28 and S13. Submissions K10, K12, K13, K19 and S19 thought it could be improved.

“Telecom believes that, generally speaking, principle 1 has worked satisfactorily in operation. It is sufficiently broad to allow the flexibility that is required in connection with normal business operations.”

- TELECOM NEW ZEALAND LTD,
SUBMISSION K12

“In many investigations Inland Revenue do source information from third parties. While in the majority of these instances the taxpayer is aware that this is taking place in others it is standard investigation technique to obtain information covertly. In many instances it is not appropriate to provide the third party with an explanation of purpose. To do so would not only reduce the effectiveness of the investigation it may well be a breach of the individual’s privacy.”

- INLAND REVENUE
DEPARTMENT, SUBMISSION K20

- information collection or to provide information on conditions;
- by constraining the circumstances in which an agency can collect information from a source other than the individual concerned, collection processes are channelled back to requests directly of the individual to which the principle 3 safeguards apply;
- collection from a source other than the individual, when the individual is in a position to provide the information directly, constitutes an affront to the individual’s autonomy - characterised by the phrase “talking about me behind my back”;
- it is an attempt to give effect to the OECD collection limitation principle which provides that personal data should be obtained, where appropriate, with the knowledge of the data subject;
- information collected might be more accurate if obtained directly from the individual concerned.

2.4.3 Nonetheless, there are circumstances where it would be unreasonable or make no sense to insist on collection of information directly from the individual concerned. For this reason, the relatively broad exceptions often apply to collections of information. Therefore, the scope of the exceptions is of as much importance as the way that the basic principle itself is framed.

2.4.4 Principle 2 does not always have a direct equivalent in information privacy laws overseas. One of its origins may have been the Information Authority’s recommendation for a collection provision which would have provided:

“A Department or Minister of the Crown or Organisation shall collect the personal information directly from the person to whom it relates except:

- (a) where the information is already publicly available; or
- (b) where the person authorises another method of collection; or
- (c) where such collection would prejudice the purpose of collection; or
- (d) where it would be of benefit to the person.”¹⁶

The Information Authority explained that “wherever possible in the interests of fairness and accuracy, information should be collected from the subject, particularly when the information may be used in decisions affecting that person.”¹⁷

2.4.5 While the Australian Privacy Act has no direct equivalent to principle 2, something similar has been proposed in the Australian National Principles for the Fair Handling of Personal Information which provides:

“Where it is reasonable and practicable to do so, an organisation should collect personal information directly from the subject of the information.”¹⁸

Exceptions

2.4.6 The exceptions to principle 2 are similar in most material respects to the sets of exceptions in principles 3, 10 and 11. The exceptions are broader than were proposed when the principle was introduced in the Privacy of Information Bill. In particular, the select committee added exceptions relating to:

¹⁶ Information Authority, *Personal Information and the Official Information Act: Recommendations for Reform 1987*, page 27.

¹⁷ *Ibid*, page 28.

¹⁸ Australian Privacy Commissioner, *National Principles for the Fair Handling of Personal Information*, February 1998, principle 1.4.

- law enforcement interests - paragraph (d)(i);
- the enforcement of a law imposing a pecuniary penalty or for the protection of the public revenue - paragraph (d)(ii) and (iii);
- the conduct of court or tribunal proceedings - paragraph (d)(iv);
- circumstances where the information will be used in a form in which individuals are not identified - paragraph (g)(i);
- information to be used for statistical or research purposes - paragraph (g)(ii); and
- exemptions obtained under section 54 - paragraph (h).

2.4.7 Although the exceptions are relatively broad - broader for instance than proposed by the Information Authority or in the Australian Privacy Commissioner's new national privacy principles - they appear to have worked satisfactorily in operation. I have no present recommendations for reform.

Notice to individual when collecting from another source

2.4.8 Where an exception applies an agency is permitted to collect information from a source other than the individual concerned. In such circumstances, the individual will not be entitled to the explanations required under principle 3 since those apply only in relation to collection directly from the individual concerned. Given the breadth of the exceptions, there may be a considerable amount of information collection activity carried out without the individual ever being made aware.

2.4.9 In some cases, this matters very little. For example, pursuant to the "publicly available information" exception a collection might be made by an agency from a "publicly available publication", such as a telephone directory. People are aware that the directory is used in such a fashion and would generally have little or no concern. However, in other circumstances, particularly where the information will be used in a way that affects their interests, the individuals affected may be very much concerned about enquiries being made and information collected without their knowledge. In only a small minority of cases, usually involving investigation which will be affected by the individual being made aware of the collection of information, is it necessary to withhold from the individual the fact that the enquiries are being made.

2.4.10 The principles could tackle the problem in one of several ways. The way that I have addressed the issue in the Health Information Privacy Code is by reducing the number of exceptions to principle 2 and by modifying principle 3 so that explanations are also given where the source of the information is the representative of the individual (a common category of health sector collections from a source other than the individual concerned). An alternative approach, taken in the Australian Privacy Commissioner's national privacy principles, is to provide that if an agency collects information from someone else that it should, where possible, make the individual concerned aware that it has done so.¹⁹

2.4.11 The new Australian principle suggests a promising approach to this problem. However, although the new Australian principles have been developed after extensive consultation with a wide range of businesses, consumers, non-profit organisations and governments, they have not as yet been implemented in an enforceable manner by law or otherwise. It is also intended that they be reviewed later this year or early next year. Therefore, it may be prudent to postpone any consideration of adopting a principle such as that until it has been further refined and implemented in Australia.

¹⁹ *Ibid*, principle 1.5. This states that "where an organisation collects personal information from a third party, it should take reasonable steps to ensure that the subject of the information is or has been made aware of the matters listed under item 1.3 above."

"There are conceivably occasions where a person's privacy could be infringed if an agency were told why the information was being collected. On the other hand there are instances when a parent is being asked for information about a child has a legitimate interest in being told what the information will be used for. The parent is providing information on behalf of an individual who is not fully able to act on its own behalf. Only in such circumstances should an agency give an explanation as to the purpose of collection."

- STATE SERVICES COMMISSION,
SUBMISSION S11

“The obligation to explain to a third party the purpose of collection may result in the inadvertent disclosure of personal information (eg locating a debtor). There should be an obligation to tell an individual that information has been collected about him or her as soon as practicable and not inconsistent with the purpose of collection.”

- KATHRYN DALZIEL,
SUBMISSION S6

2.4.12 In consultation I sought views on whether principles 2 or 3 should be modified to oblige agencies to explain the purpose for which information is required when collecting personal information from someone other than the individual concerned. The question attracted 24 submissions. Fourteen were in support of the proposed change²⁰ with 9 opposed.²¹ Submissions both in favour and opposed to the proposition mentioned that explanations as to the purpose for collecting information from a third party would be appropriate in some circumstances but not others.²² A common refrain was that telling a third party the purpose of collection might diminish the individual’s privacy in some circumstances. One submission suggested that the agency collecting the information should not be obliged to explain the purpose but the recipient of the request, if it actually released the information, should tell the individual that it had done so (submission K21). Others suggested that it would be appropriate for an explanation as to the purpose of the request to be provided where the collection was from a representative of the individual, that is a person who stands in the place of the individual with a responsibility to protect the individual’s interests.²³

2.4.13 The discussion paper offered an alternative that principle 2 or 3 be amended to require an agency to tell the individual concerned if the agency intended to collect information from a third party. Again, responses were relatively evenly split. Fourteen submissions said that this should be required²⁴ while 11 submissions opposed such a requirement.²⁵ It is plain that a suitable rule, appropriate to all circumstances, might be difficult to achieve. The matter should be revisited at a future date when experience under the proposed Australian principle can be evaluated.

2.5 PRINCIPLE 3 - Collection of information from subject

2.5.1 Principle 3 is one of the most important provisions in the Privacy Act. It brings together features of several of the OECD principles. Underlying the principle are ideas of openness: that collection of personal information should be done with the knowledge or consent of the individual concerned, that the purposes for which information is collected should be specified no later than the time of collection and subsequent use limited to fulfilment of those and compatible purposes, and there should generally be transparency about information collection policy and individual participation in that process.

2.5.2 The principle requires that where an agency collects personal information directly from the individual concerned, the agency take reasonable steps to ensure that the individual is aware of certain matters. Those steps are to be taken before the information is collected or, if that is not practicable, as soon as practicable thereafter. There are some exceptions where the individual does not have to be made aware of the various matters.

Explanations required by principle 3(1)

2.5.3 The principle requires individuals to be made aware of a number of items:

- the fact of collection;
- the purpose for which the information is being collected;
- the intended recipients;
- the name and address of the agency collecting and that will hold the information;

²⁰ Submissions K3, K8, K11 - K13, K18, K19, K25, K28, S21, S24, S36 and S42.

²¹ Submissions K9, K14, K20, K21, S6, S13, S15, S25 and S56.

²² See, for example, submissions K12, K18, K19, K20, K28, S6, S11, S15 and S25.

²³ See, for example, submissions K28, S6, S11 and S15.

²⁴ Submissions K3, K10, K11, K12, K18, K19, K25, K29, S6, S19, S21, S24, S36 and S42.

²⁵ Submissions K8, K9, K13, K14, K20, K21, K28, S13, S15, S25 and S45.

- any law authorising or requiring the collection and whether that law makes the supply of the information voluntary or mandatory;
- the consequences if the request for information is not provided; and
- the rights of access and correction.

2.5.4 The required explanations in principle 3(1) remain the same as those introduced in the Privacy of Information Bill. I have compared the principle to similar requirements appearing in other privacy laws and it is broadly similar to most and, from an individual’s perspective, better than many in terms of the breadth of useful information required to be conveyed. For example the absence in the Australian Privacy Act of an equivalent to our principle 3(1)(f) has been described as a “significant gap” in the Australian privacy principles.²⁶

2.5.5 A few laws require other details to be provided. For example, the British Columbia law requires that the individual concerned be made aware of:

“The title, business address and business telephone number of an officer or employee of the public body who can answer the individual’s questions about the collection.”²⁷

While that requirement is pitched at a level that is useful for an individual I do not propose it for our own principle 3. The British Columbia Act primarily applies to the provincial and local government sectors. With that limited application a precise requirement of the type described is probably appropriate and useful. With a far larger range of public and private bodies covered by our Act I prefer to keep the principle at the present level of generality requiring simply the name and address of the relevant agency.²⁸

2.5.6 Some overseas principles indicate that the individual should be made aware of certain information handling policies or practices of the agency. For example, the “notice principle” in the National Information Infrastructure Principles (USA) states:

“Information users who collect personal information directly from the individual should provide adequate, relevant information about what steps will be taken to protect its confidentiality, integrity and quality.”²⁹

2.5.7 The NII principles have not been implemented in the USA in an enforceable fashion and therefore do not offer a useful precedent to draw on. By contrast, the Hong Kong law has a principle, not linked to collection of information from the individual concerned, which requires certain information on agencies’ practices to be made available. It states:

“PRINCIPLE 5 - Information to be generally available
All practicable steps shall be taken to ensure that a person can:
(a) ascertain a data user’s policies and practices in relation to personal data;

²⁶ Australian Privacy Commissioner, Privacy Protection in the Private Sector: Response to Discussion Paper issued by the Attorney-General, December 1996, page 6.

²⁷ Freedom of Information and Protection of Privacy Act 1992 (British Columbia), section 27(2).

²⁸ Nonetheless, a provision which might be worth considering at a later date, if successfully implemented in Australia, is the simple formulation in the Australian National Principles for the Fair Handling of Personal Information which refers to “the identity of the organisation and how to contact it” (principle 1.3(a)).

²⁹ Privacy Working Group, Information Policy Committee, Information Infrastructure Task Force, “Privacy and the National Information Infrastructure: Principles for providing and using personal information”, final version 6 June 1995, principle IIB.

“The items currently listed in (a) to (g) reflect an appropriate balance between ensuring that individuals are protected and not imposing undue burdens on agencies. The items currently required in principle 3 explanations are sufficient to allow individuals to exercise their rights in relation to their personal information.”

- MINISTRY OF JUSTICE,
SUBMISSION K28

- (b) be informed of the kind of personal data held by a data user;
- (c) be informed of the main purposes for which personal data used by a data user are or are to be used.”³⁰

2.5.8 There was some support in submissions for a principle, not linked to collection, to require openness regarding agency information practices.³¹ I suggest that such matters might better be dealt with in the framework of our law within specifically issued codes of practice rather than a new principle. That would allow for any obligations to be particularised to a sector or type of information or activity. As this would not necessarily be able to be achieved easily by simply modifying an existing principle I suggest that the power for issuing codes of practice should be broadened to expressly refer to the matter detailed in principle 5(a) of the Hong Kong law.



RECOMMENDATION 18

Section 46(4) should be amended to provide that a code of practice may require an agency to take all practicable steps to ensure that an individual may ascertain the agency’s policies and practices in relation to particular personal information.

2.5.9 Most submissions were opposed to adding any further explanations to principle 3(1)³² or indeed to making any changes to items (a) to (g) of principle 3(1).³³ However, a few submissions favoured change including that:

- consideration be given to simplifying or clarifying the explanations;³⁴
- item (b), which simply refers to “the purpose”, ought to be reconciled with principle 3(4)(d) which refers to “the purposes”.³⁵

Purpose or purposes

2.5.10 Principle 1 speaks of the collection of personal information for a “purpose”. It has been suggested during consultation, and earlier when the Privacy of Information Bill was before the select committee, that it is confusing to refer solely to single “purpose” when there might be more than one purpose of relevance. The singular is also used in principles 1(a) and 8. Some of the other principles, and the exceptions to the principles, use “purposes”.

2.5.11 The proposition to replace the reference to “purpose” by “purpose or purposes” was rejected by the select committee because on normal statutory interpretation the term would be read that way in any case. In particular, section 4 of the Acts Interpretation Act 1924 states:

“Words importing the singular number include the plural number, and words importing the plural number include the singular number.”

2.5.12 I think that the position will be plainer for users of the statute if the phrase “purpose or purposes” is substituted. My concern extends to lay people who are not familiar with normal rules of statutory interpretation.

³⁰ Personal Data (Privacy) Ordinance 1995 (Hong Kong), Schedule 1.

³¹ Submissions R4, R5, R6, R8, R12, S24, S42 and S56 were in favour. Submissions R3, R13, S3 and R14 were opposed.

³² Twelve of the 15 submissions opposed adding further items (K8, K9, K12, K14, K18, K19, K21, K25, K27, K28, S11 and S13). Submissions K11 and S42 liked the British Columbia requirement to give a telephone number with K13 favouring greater advertisement to individuals of the ways to contact a privacy officer.

³³ Thirteen of the 18 submissions on this point saw no case for change (see submissions K8, K9, K11, K12, K14, K18, K20, K25, K27, K28, S6, S11 and S13).

³⁴ Submissions K6 and S42.

³⁵ Submission S19.

“Overall the items listed are useful and give the information giver certain rights of control and protection.”

- NEW ZEALAND COLLEGE OF MIDWIVES, SUBMISSION K13

“We consider that principle 3(1) is too unwieldy as it is without needing to expand on the amount of information than an agency should provide.”

- BAYNET CRA LTD, SUBMISSION K21

**RECOMMENDATION 19**

Information privacy principles 1, 3(1) and 8 should be amended to substitute the phrase “purpose or purposes” for the word “purpose”.

Principle 3(2) and (3)

2.5.13 Principle 3(2) makes it clear that the steps required to be taken in principle 3(1) must be taken before the information is collected but that if that is not practicable the steps are to be taken as soon as practicable thereafter. This provision is copied from principle 2 of the Australian Privacy Act.

2.5.14 Principle 3(3) provides that an agency is not required to take the steps referred to in principle 3(1) if the agency has taken those steps in relation to the collection from that individual of the same or similar information on a recent previous occasion. This subclause is not taken from the Australian Privacy Act and did not appear in the Privacy of Information Bill as introduced. It was added by the select committee to reduce, in a modest way, potential compliance costs for agencies. It also ensures that unneeded and unwanted explanations are not unnecessarily repeated.

Exceptions

2.5.15 Principle 3(4) contains exceptions which are almost identical to exceptions found in principle 2, 10 and 11. The list is far more extensive than was originally contained in the Privacy of Information Bill, which solely contained an exception similar to the present exception (d). The equivalent principle in the Australian Privacy Act contains no exceptions at all, with resultant emphasis being placed upon the “reasonableness” or “practicability” of giving explanations in difficult circumstances.

2.5.16 Approximately two thirds of the 19 submissions received in relation to principle 3(4) expressed comfort with the present exemptions. The remainder were concerned about the exceptions contained in principle 3(4)(a) and 3(4)(f)(ii) relating to individual authorisation, and statistical and research purposes, respectively.

Authorisation for non-compliance

2.5.17 Principle 3(4)(a) permits an agency to dispense with explanations anticipated by principle 3(1) when “non compliance is authorised by the individual concerned”. This exception could be problematic if authorisations are sought on standard forms where there is imbalance in bargaining position between individual and agencies. The exceptions might even be characterised as an authorisation to “contract out” of one of the key provisions in the Act.

2.5.18 In order for an authorisation to be meaningful in terms of the Act’s principles it should be an *informed* authorisation which would be unlikely to be the case if the individual is denied the explanations anticipated by principle 3(1). It also upsets the scheme of the principles, such as those governing use and disclosure, if the purpose of collection is not specified at the outset. The complementary nature of the principles is upset by this exception.

2.5.19 I have concluded that principle 3(4)(a) should be repealed. It is an unusual provision not generally found in the equivalent exceptions in overseas privacy laws. I can find no justification for it within the OECD guidelines on which the Act is based.

**RECOMMENDATION 20**

Information privacy principle 3(4)(a) should be repealed.

Statistical or research purposes exception

2.5.20 Concern has also been expressed in relation to the exception contained in principle 3(4)(f)(ii) whereby agencies need not make individuals aware of the matters in principle 3(1) where the information:

“It is difficult to justify an individual authorising a waiver of the explanation required to enable them to make informed decisions about their personal information. In order for an authorisation to be meaningful in terms of the Act’s aims and principles, it should be an *informed* authorisation.”

- MINISTRY OF JUSTICE, SUBMISSION K28

“Will be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned.”

2.5.21 I recognise an important public interest in statistical and research purposes. The exceptions which exist in principles 2, 10 and 11 are, to my mind, appropriate and essential features of the scheme of the Act. However, I am not convinced that the gathering of statistics, or the fact that the objective is research, justifies an exception to principle 3(1) where the collection of *personal information is directly from the individual concerned*. I emphasise that principle 3:

- concerns only the collection of “personal information”; and
- applies where the collection of the information is “directly from the individual concerned”.

An exception is not needed where:

- collection is from individuals whose identities are not known (such as anonymous street interviews where identifying details are not taken); or
- collection is from sources other than the individual concerned (such as research concerning existing records).

2.5.22 Collection of information directly from the individual for the purposes of research or statistics will typically involve an interview or a request for the individual to complete a form. I cannot see that there is anything inherent in the nature of research, or the collection of statistics, which should relieve an agency collecting personal information from explaining, amongst other things:

- the purpose of the collection;
- the intended recipients;
- the identity of the agency that is asking the questions;
- whether the supply of the information required under law is voluntary or mandatory.³⁶

2.5.23 Nor, do I believe that any significant difficulty should be caused to legitimate and ethically conducted research or statistics gathering in providing such explanations. I should add that in particular circumstances there may be a reason to rely upon one of the other exceptions to delay the giving of certain explanations until the collection is complete. For example, responses to a survey which are supposed to be unprompted might be affected if the name of the agency which has commissioned the research, and which is to be the recipient of the information, is given out in advance of the questions being posed.³⁷ In such cases, I expect that principle 3(2) and 3(4)(d) may be relied upon so that the requisite explanation is given after the interview or form is completed.

2.5.24 I received a helpful submission from the Association of Market Research Organisations (AMRO) which explained its position and the importance attached to the relevant exemptions to the information privacy principles. While it opposed the removal of the exemptions I believe that its concerns will be largely met so long as the relevant exceptions to principles 2, 10 and 11 are retained. In fact, it appears that the requirements of AMRO’s Code of Practice require members to comply with obligations which are remarkably similar to principle 3 in various respects. For example, the code³⁸ provides as follows:

“Respondents’ cooperation in a market research project is

³⁶ There would be few statistical or research collection of personal information which are conducted under law and which are mandatory. The prime example would be those undertaken by Statistics New Zealand and I have little doubt that the practice of that agency would be to tell recipients of the sort of matters specified in principle 3(1).

³⁷ I expect that in many cases no actual personal information will be transferred to the commissioning organisation but instead just the statistical research results.

³⁸ Code of Practice of the Market Research Society of NZ Inc, January 1995. This is an industry code of conduct, not a code issued under the Privacy Act.

“It is not appropriate for any person to be expected to disclose personal health information without knowing its use. While there is definite benefit in the gathering of statistical or research data it must never be done without disclosure of its use to the individual who volunteers that information.”

- NZ COLLEGE OF

MIDWIVES, SUBMISSION K1.3

entirely voluntary at all stages. They must not be misled when being asked for the cooperation.” (Article 3)

“If the respondent is supplying information not in a private capacity but as an officer of an organisation or firm it may be desirable to list the respondent’s organisation in the report. The report, shall not, however, enable any particular piece of information to be related to any particular organisation or person, except with prior explicit permission from the relevant respondent, who shall be told of the extent to which it will be communicated. This requirement does not apply in the case of secondary analysis of published data.” (Article 5)

“The researcher must avoid unnecessary intrusions on respondents’ privacy”. (Article 6)

“Respondents’ anonymity must always be strictly preserved unless they have explicitly agreed to the contrary. The researcher must ensure that the information they provide cannot be linked to specific individuals or organisations without such permission. It is the researcher’s responsibility to inform clients of respondents’ anonymity rights”. (Article 7)

“In any case where respondents are asked for permission to disclose their name and/or address to anyone outside the research agency:

- (a) the respondent must first be told to whom the information would be supplied and the purposes for which it will be used, and also;
- (b) the researcher must ensure that:
 - (i) the information will not be used for any non-research activity;
 - (ii) the information will not be published in a form that could reasonably be expected to identify the respondents; and
 - (iii) the recipient of the information has agreed to conform the requirements of this code.” (Article 8)

“Respondents must be told at the time of the interview when observational recording techniques are to be used, except when these are used in a public place. If a respondent so wishes, the record or relevant section of it must be destroyed or deleted. Respondents’ anonymity must not be infringed by use of such methods”. (Article 10)

“Respondents must be able to check without difficulty the identity and bona fides of the researcher and to obtain an answer to any reasonable query about the purposes and content of the research. Each interviewer must be able to be identified in a way that specifies his or her name and organisation. The name and address/telephone number of the research company must be made available to the respondent at the time of the interview.” (Article 11)

2.5.25 A further difficulty with the exception is that it does not make clear what it is to “publish” the information. Clearly the constraint on publishing information in a way that identifies the individual is an important protection. However, it

may well be that the disclosure of the information from the agency which collects it, as part of a research or statistical project, to another agency, such as an agency which has commissioned the research, may not be characterised as “publication”. If that view were to be taken it would mean that the individual is completely left without protection in a privacy sense and is in the dark as to why information was collected and who will get hold of it. If the exception were to be retained it ought to be narrowed so that it may only be relied upon if the information from which individuals may be identified is to remain solely with the agency that collects the information. However, in my view the exception should be repealed totally rather than simply refashioned in that way.



RECOMMENDATION 21

Information privacy principle 3(4)(f)(ii) should be repealed.

2.6 PRINCIPLE 4 - Manner of collection of personal information

2.6.1 Principle 4 is relatively brief and straightforward and prohibits the collection of personal information by an agency by unlawful means or unfair or unreasonably intrusive means. The principle seeks to give effect to the OECD collection limitation principle and its constituent parts are drawn from information privacy principles 1(2) and 3(d) in the Australian Privacy Act.

2.6.2 The principle has featured in a number of complaints to my Office. Those reported in case notes to date have included:

- a private investigator, in breach of the Private Investigators and Security Guards Act 1975, photographing another person without that person’s prior written consent (case note 3734);
- hidden video camera surveillance in a workplace locker-room (case note 632);
- a private investigator posing as a potential guest in accommodation premises (case note 6314);
- a police officer telephoning a school to seek children’s address on the pretext of returning stolen property whereas in fact in context of deportation of father (case note 11536);
- a private investigator using a ruse of being a potential buyer to enter a home and videotape the occupants (case note 14824).

2.6.3 I have no suggestions for amendment of principle 4 which was considered by most submissions to have worked well.³⁹

2.6.4 The Complaints Review Tribunal has not yet had the opportunity to consider principle 4 although interestingly the courts, in their criminal jurisdiction, have. The case of *R v Wong-Tung*⁴⁰ concerned the lawfulness of attaching a telephone analyser to a telecommunications network. A telephone analyser is a device which enables the recording of data generated as a result of telecommunications made using a telephone line. The data recorded is restricted to information about the telecommunication (such as the number called, the time called, and the duration of the call) and does not include the content of the telecommunications.

2.6.5 The practice of attaching telephone analysers in the course of criminal investigations had grown up since the 1980s without any regulation, in contrast to the strong controls on the interception of the content of private communications. From 1993 the Privacy Act essentially regulated aspects of the practice which was not entirely satisfactory from the perspective of telecommunication companies, law enforcement agencies or the privacy interests of individuals.

³⁹ See submissions K8, K9, K12, K13, K14, K18, K19, K21, K25, K27 and K28.

⁴⁰ (1996) 2 HRNZ 272. It is unnecessary to examine the facts and findings of that case here.



“One of the key positives of principle 4 is the general nature in which it is prescribed. It is not burdened with large numbers of exceptions and restrictions. It should be maintained in the current format.”

- INLAND REVENUE

DEPARTMENT, SUBMISSION K20

Accordingly, I welcomed the recent enactment of provisions prohibiting the attachment of telephone analysers except with a judicial “call data warrant”.⁴¹ I consider that something similar ought to be considered for covert video surveillance for law enforcement purposes as it is unlikely that principle 4 or the other principles will be sufficient to appropriately constrain or control the activity which leads to similar strong privacy concerns.



RECOMMENDATION 22

Consideration should be given to establishing a judicial warrant process in relation to the use of covert video surveillance in the investigation of offences.

2.7 PRINCIPLE 5 - Storage and security of personal information

2.7.1 Principle 5 is derived from the OECD security safeguards principle which provides:

“Security safeguards principle

Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.”⁴²

2.7.2 Principle 5 is closely modelled on principle 4 of the Australian Privacy Act. In addition to paragraph (a), which closely follows the approach of the OECD security safeguards principle, there is, in both the New Zealand and Australian Acts, a second paragraph placing security obligations on agencies where information is given to a person in connection with the provision of a service to the agency.

2.7.3 Principle 5 is clearly expressed and easily understood by agencies. It does not appear to have caused significant interpretational problems in operation.

Recent international security safeguards developments

2.7.4 Since the 1980 OECD guidelines were released there has been a significant amount of work undertaken internationally on refining information security principles. In 1992 the OECD released its Guidelines for the Security of Information Systems (“the 1992 Guidelines”). These built upon the security safeguards principle in the 1980 Guidelines and contained 8 further principles, being the:

- accountability principle;
- awareness principle;
- ethics principle;
- proportionality principle;
- periodic reassessment principle;
- multi-disciplinary principle;
- integration principle;
- democracy principle.

2.7.5 The 1992 Guidelines were finalised after the Privacy of Information Bill had been drafted and introduced into Parliament and after the Privacy Commissioner Act 1991 had been enacted. Accordingly, those guidelines did not feature in the drafting of the legislation.

2.7.6 The 1992 Guidelines provide a valuable elaboration of the 1980 Guidelines and offer a recommended approach to issues concerning the security of information systems. I have concluded that there is no particular need to refer to them explicitly in the Act. I already have authority to take account of the 1992 Guidelines pursuant to section 14(b) and (c). I encourage agencies, especially public bodies and industry groups, to consider them in their development of policies concerning the security of information systems.

⁴¹ See report by the Privacy Commissioner to the Minister of Justice in respect of Part X of the Harassment and Criminal Associations Bill amending the Telecommunications Act, Telephone Analysers and Call Data Warrants, 10 September 1997.

⁴² OECD Guidelines, clause 11.

- 2.7.7 Another relevant OECD development concerns cryptography. In 1996 the OECD released guidelines for cryptography policy which contained within them a set of principles.⁴³ As the guidelines are very recent it is difficult to gauge how influential they will be throughout the OECD and international community. I am unaware of any country having yet legislated on the basis of the OECD cryptography guidelines (although some countries have legislated in respect of cryptography policy). Cryptography has become central to aspects of the debate over security of personal information and if New Zealand were to adopt a more restrictive policy in this area it would be desirable to consider the privacy and Privacy Act implications. The OECD work would be valuable in that context. In particular, I highlight principles 2 and 5 of those guidelines which provide:

“2. Choice of cryptographic methods

Users should have a right to choose any cryptographic method, subject to applicable law.

“5. Protection of privacy and personal data

The fundamental rights of individuals to privacy, including secrecy of communications and protection of personal data, should be respected in national cryptography policies and the implementation and use of cryptographic methods.”

- 2.7.8 Although I sought views on the issues in the consultation I do not see this review as being an appropriate vehicle to take any initiatives in respect of cryptography. Principle 5 is intentionally silent as to technical means of achieving adequate security as these will vary over time. It is unlikely that reference to a specific technique or technology, such as cryptography, would be appropriate in this principle. Nonetheless, there is a strongly held view amongst many people interested in privacy that individual access to cryptography technology is likely to be an essential means to protect privacy as we move into the Twenty-first Century and the global information society.
- 2.7.9 Other sets of privacy principles have also tackled security issues in new ways. The EU Directive on Data Protection deals with “confidentiality of the processing” and “security of processing” in articles 16 and 17 in ways which differ slightly from our own principles. The EU Directive also differs in relation to “sensitive categories of data” and the “transfer of personal data to third countries”. I deal with the latter issue in detail at paragraph 2.18.
- 2.7.10 In the USA the National Information Infrastructure principles took a novel approach to information security. They emphasised the empowerment of individuals to utilise technology to safeguard their own data. One part of the “empowerment principle” stated:

“Individuals should be able to safeguard their own privacy by having the opportunity to use appropriate technical controls, such as encryption, to protect the confidentiality and integrity of communications and transactions.”

- 2.7.11 The empowerment principle also stated that individuals should be able to safeguard their own privacy by having the opportunity to remain anonymous when appropriate. Anonymity is often the most effective security safeguard that individuals can adopt. Pseudonymity is also a very effective means for enhancing privacy particularly when individuals participate in transactions. Pseudonymity provides for an identifier to be assigned to an individual as a party to a transac-

“The Act should not move away from the concept of statements of principle to also prescribe the methodology by which those principles may be implemented. Legislation that has set out to define methodology has become rapidly dated as technology has changed and that the rate of technological change continues to increase. If, however, it is considered necessary to legislate on the subject of cryptology, the Bureau would take the view that the Privacy Act is not the appropriate vehicle by which to do so.”

- GOVERNMENT

COMMUNICATIONS SECURITY BUREAU,

SUBMISSION K4

⁴³ OECD, Recommendations of the Council concerning Guidelines for Cryptography Policy, 27 March 1997.

tion which is not, in the normal course of events, sufficient to associate the transaction with a particular human being. A transaction is pseudonymous in relation to a particular party if the transaction data contains no direct identifier for that party. Nonetheless, the identity of that party can be established, in appropriate circumstances by, for example, bringing together partial identifiers which have been stored separately by two or more organisations. Another approach is for an indirect identifier to be stored with the transaction and a cross index to be held which would enable the person's real identity to be divulged in specified circumstances subject to organisational, technical and possibly legal, safeguards.⁴⁴

- 2.7.12 I have no recommendations for amendment to principle 5. It has worked well and applies an appropriate standard for information security to take account of changing circumstances and the availability of new technologies. However, as the preceding discussion has suggested there is a lively international debate about information security, particularly as regards cryptography policy. The potential of privacy enhancing technologies has also focused attention on the possibilities for anonymous or pseudonymous transactions to enhance privacy. Developments in this area may not require any change to principle 5 but with the pace of change in this area being quite rapid I expect that the matter will require re-examination at the next periodic review of the Act.

Browsing or inspection of information

- 2.7.13 I have outlined elsewhere that an issue has arisen overseas, and in New Zealand, as to whether “browsing” constitutes a “use” of information under a privacy or data protection law. Browsing of information typically involves employees, who are authorised to have access to an agency's information holdings in connection with their employment on their employer's business, inspecting or browsing through files for no legitimate purpose. Sometimes employees are simply curious. Others wish to find out information about friends, family members, acquaintances or enemies. In some cases, the browsing is a precursor to the improper disclosure of the information or its sale. This can be a particular issue in relation to large databases such as those maintained by the Police, Income Support, CYPFS, and public hospitals, where it can be difficult to limit access to small numbers of staff.
- 2.7.14 Browsing is seen as an affront to privacy of the individuals concerned but it is not always easy to characterise the practice as a breach of the privacy principles. This is principally because it is debatable whether simply reading or inspecting information, but not otherwise acting upon it, constitutes a “use” of the information. Accordingly, one possible response is to define “use” in a way that encompasses the practice. I have recommended elsewhere that this be considered.⁴⁵
- 2.7.15 However, another way of tackling the issue may be to modify information privacy principle 5 so as to make it plain that agencies are required to safeguard personal information against browsing. The present obligations in information privacy principle 5 relate to loss, access, use, modification, disclosure or other misuse. The practice of browsing does not concern loss or modification of information. Generally it does involve access to information but typically the browser is a person authorised to have access to the agency's records but is doing so for purposes that have not been authorised and which are not the agency's purposes. Accordingly, the obligations relating to access are arguably not enough of themselves. Typically it is alleged that browsing does not involve use or disclosure of information - or at least any use or disclosure which can be

⁴⁴ This description of pseudonymity is taken from Dr Roger Clarke, “The Scope for Transaction Anonymity and Pseudonymity”, Fifth Conference on Computers, Freedom and Privacy, 1995.

⁴⁵ See paragraphs 1.4.103 - 1.4.111 and recommendation 16.

“New Zealand’s original principle 5 is too vague to be of much value today. Electronically stored information require safeguards that are specific to both the storage method and the system that is being used. Specific aspects of the OECD’s Guidelines for the Security of Information Systems should be included in principle 5 and not just referred to elsewhere in the Privacy Act.”

- DR LALITA RAJASINHAM, VICTORIA UNIVERSITY, SUBMISSION K1

proved. It is possible that the practice constitutes “other misuse” although that in itself may be dependent upon whether one considers browsing as “use”.

- 2.7.16 I suggest that the practice could be tackled by inserting the word “browsing” or “inspection” in principle 5(a)(ii) which will oblige agencies to take safeguards against the practice.



RECOMMENDATION 23

Information privacy principle 5(a)(ii) should be amended by inserting the word “browsing” or “inspection”.

2.8 PRINCIPLE 6 - Access to personal information

- 2.8.1 All jurisdictions which have specific privacy legislation include within that a right of access by individuals to information held about them. Principle 6 provides that right of access and it gives effect, in part, to the OECD “Individual participation principle”.

- 2.8.2 The right of access is important in a variety of ways. Lying behind privacy legislation is a recognition of an individual’s entitlement to some degree of personal autonomy. That autonomy would be illusory in many cases unless the individual can see what information is held for potential use by others. Another reason for the right of access is because of the concern that personal information to be used should be accurate and possibly the best way of ensuring such accuracy is to let the individuals see it and point out any errors. It provides some measure of accountability by agencies to the individuals whose personal information they hold and may use. Finally, an individual’s right of access tends to make other aspects of the information privacy principles self-policing. Objectionable handling of personal information might tend to come to light through the individual securing access either in the hands of the agency concerned or in the hands of another agency to which the information has been passed.

Legislative history

- 2.8.3 The Official Information Act 1982 gave everyone the right to have access to information which was held by those public sector bodies covered by the legislation. This initially was the core public service.⁴⁶ The list of bodies covered has been broadened subsequently with the main extension made in 1987 to, including others, universities, schools and public hospitals. Also in 1987 the Local Government Official Information and Meetings Act was enacted which is both a freedom of information law and a “sunshine” law (the latter feature constraining local authorities in their ability to meet in secret).
- 2.8.4 Within the overall right of access contained in the official information statutes was a special right for individuals to have access to personal information held about themselves by any of the bodies covered. There are fewer grounds for withholding such information from the individual concerned. No charge was permitted to be made for such access.
- 2.8.5 In 1993 the individual right of access to personal information was transferred to the Privacy Act and at the same time it was extended to the private sector. One significant difference between the sectors was that, in order to minimise the cost to business, private sector agencies were permitted to recover at least some of their costs from the requester. By and large, the permissible grounds under the Privacy Act upon which any agency can decline to disclose to the requesting individual what it holds about them are the same as those previously applicable under the official information statutes.

⁴⁶ Essentially, the initial application of the official information legislation corresponded to those agencies defined as a “Department”, “Minister” or “Organisation”, in section 2.

- 2.8.6 Since 1993 many thousands of New Zealanders have exercised access rights under information privacy principle 6. It is not possible to put a precise figure on the number of requests as the legislation, and the Official Information Act which preceded it, puts an emphasis upon simple procedures and the avoidance of unnecessary formalities. Accordingly, access requests need not utilise a special form or be in writing, be routed through a special officer, or be logged or counted in any particular fashion. No statistics are kept as to access requests made. However, statistics are kept in relation to complaints lodged with my office. Complaints which include access are the largest single category of complaints making up approximately 40% of the total. Further details about the number of complaints received since 1993 can be found at Appendix J. Similarly, proceedings before the Complaints Review Tribunal have predominantly concerned refusal of access requests.
- 2.8.7 There was a great deal of interest in the issues of access to personal information in the consultation process. Fifty submissions were received on the access and correction discussion paper, the most for any of the discussion papers.
- 2.8.8 The right of access to personal information is widely supported and is recognised to be an important and powerful individual right. Accordingly, in my review most of the attention in this context has been towards the detail of the access regime, notably aspects of the permitted withholding grounds and the procedural provisions for giving access, rather than the right itself. Most submissions considered principle 6 to have operated satisfactorily.⁴⁷ The issues raised and examined primarily concerned the reasons for withholding information and the procedural provisions. These are discussed in respect of Parts IV and V elsewhere in this report.
- 2.8.9 The right of access is also associated strongly with procedural fairness. Many people aggrieved at some action, or lack of action, about a matter concerning them, obtain a real satisfaction from being able to access relevant information. This accountability shines a light into what may have hitherto been dark places and can lead to a change of approach and a greater sense of responsibility by agencies.

2.9 PRINCIPLE 7 - Correction of personal information

- 2.9.1 Principle 7 provides that, where an agency holds personal information, the individual concerned has a right to request correction of the information and, if the correction is not made, to request there be a statement attached to the information that correction was sought but not made.
- 2.9.2 Principle 7 shares a similar legislative history to principle 6. The right was originally contained in the official information statutes and therefore has existed in the public sector since the 1980s. The entitlement to seek correction of personal information also gives effect to the final part of the OECD “Individual participation principle” which indicates that an individual should have the right:
- “to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.”
- 2.9.3 A number of principle 7 complaints have been brought to me. The most common situation concerns information held on the files of credit reporting agencies which is alleged by an individual to be inaccurate, incomplete or misleading.⁴⁸ The Complaints Review Tribunal has also considered several cases involving the principle.⁴⁹

⁴⁷ See submissions K8, K9, K11-K14, K18, K21, K25 and K27.

⁴⁸ See, for example, case notes 451, 613, 909 and 1827.

⁴⁹ See, for example, *Powell v Special Education Service*, Complaints Review Tribunal, 26 July 1996, Decision No CRT 26/96, *Adams v Police*, Complaints Review Tribunal, 12 June 1997, Decision No CRT 16/97.

“Although any “non-business” cost is an imposition on business, to date it does not appear that compliance costs are excessive.”

- NZ EMPLOYERS FEDERATION,
SUBMISSION WX3

- 2.9.4 Most submissions on the subject considered that principle 7 had operated adequately.⁵⁰ However, two commented that:
- the principle should state that no charge may be made for an individual seeking to have information corrected (submission K11);
 - the concept of “attaching” a statement to information under principle 7(3) should be made more clearly applicable to information in electronic form (submission K12).
- 2.9.5 The first point has some validity and I address it in recommendation 65. However, with respect to the second point I consider that the Act works satisfactorily in relation to “attaching” a statement to electronic data notwithstanding that there may be a semantic issue as to whether one can truly “attach” a piece of data to another in an electronic environment. Agencies usually include the statement within the same electronic document or databank or they attach a “flag” of some sort which refers users to a hard copy record or to the location of the electronic record.
- Obligation to advise of right under principle 7(1)(b)*
- 2.9.6 Principle 7(1) confers two entitlements on individuals:
- (a) to request correction of personal information held by an agency; and
 - (b) to request that there be attached to the information a statement of the correction sought but not made.
- Principle 7(2) to 7(5) explains how the entitlement is to be acted upon by an agency. The two parts of principle 7(1) usually work adequately together because an agency which refuses to act upon a request for correction will normally volunteer to the requester, when explaining that the correction will not be made, that the requester may ask for a statement to be attached for the unchanged information. Principle 7(3) seems to make clear that the agency’s obligation to attach a statement is activated only upon a request by the individual concerned. Typically, this will be a second request by the individual unless they have earlier asked for a correction and, in lieu, for the attachment of a statement.
- 2.9.7 I suggest that the principle should be amended so that an agency is obliged to inform requesters of the entitlement to request that a statement be attached. I do not think it is necessary to go so far as to oblige agencies to actually attach such a statement in the absence of a further request from the individual although I note that this was the obligation in the corresponding provision in the Official Information Act that formerly related to correction of information.⁵¹ There was a fair measure of support for such a proposal in submissions.⁵²



RECOMMENDATION 24

Information privacy principle 7 should be suitably amended so that agencies are obliged to inform requesters, in cases where the agency is not willing to correct information, that they may request that a statement be attached to the information.

Preventing use of information for purposes of direct marketing

- 2.9.8 Direct marketing continues to be the subject of a stream of enquiries to my office. The issue is frequently couched in terms of a failure of an agency to act upon a request to delete a person’s name from a mailing list. As “correct” includes the alteration of personal information by way of deletion it is understandable that the matter is sometimes asserted to be an entitlement conferred by principle 7.

⁵⁰ See submissions K8, K9, K11, K13, K14, K18, K21, K25 and K27.

⁵¹ Official Information Act 1982, section 26(1)(b).

⁵² Twelve submissions considered that principle 7 should be more specific as to an agency’s obligation to consider and give effect to a request for correction (see submissions L2, L4, L5, L7, L13, L14, L19, S2, S7, S36, and S45).

- 2.9.9 The principle does entitle individuals to *request* deletion of details from an agency’s mailing list and to *oblige* the agency to take a decision to accept or deny the request. However, it is unlikely that an agency can be *obliged* to delete accurate information under the principle.
- 2.9.10 The principle has as its primary focus the correction of inaccurate information rather than the deletion of information which it is alleged should not be used for a particular purpose. In that sense, it might be characterised as a data quality entitlement rather than a limit upon use. One might therefore argue that principle 7 is appropriately used for removing a name from a marketing list where the individual’s details were placed on the mailing list through error but not because the details were obtained in breach of principle 3 or 11.
- 2.9.11 However, I would like to move the issue beyond the interpretation of principle 7 as it presently appears onto the issue of whether individuals should be entitled to be removed from direct marketing lists. There was support for this proposal in submissions.⁵³
- 2.9.12 An entitlement to be taken off lists used for direct marketing purposes would be easy for individuals to exercise. It would be a fairly straightforward request for agencies to respond to and to be reviewed on a complaint. At present, direct marketing complaints could involve an elaborate inquiry into the circumstances in which an individual’s details came to be placed on an agency’s marketing list. In essence this involves a check of compliance with principles 1 to 4 and possibly 10 and 11. This can be done but it will usually be more straightforward to simply take the person’s name off the list. This is how such customer complaints are frequently resolved.
- 2.9.13 Direct marketing complaints are some of the most common allegations of use of personal information obtained for one purpose for another purpose. The harm or detriment suffered by individuals is undoubtedly at the low end of the scale. However, while the harm may be minimal at an individual level, the quantity of direct marketing means that a single mail-shot may cumulatively affect and irritate many thousands of individuals and therefore be a significant breach of the collection, use and disclosure principles. In my view, the problem should be addressed with a comparatively simple mechanism which, consistent with the information privacy principles, gets to the heart of the consumer dissatisfaction. The answer is to empower individuals to demand that their details be removed from, or blocked on, lists held for direct marketing purposes. This is the approach required of members of the Direct Marketing Association by the Association’s rules. However, the DMA’s voluntary scheme has not been successful because amongst other things, it is confined to members and lacks enforcement mechanisms.
- 2.9.14 This is the approach of in the EU Directive on Data Protection which provides in article 14(b):

“The data subject’s right to object

Member states shall grant the data subject the right:

- (b) to object on request, and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing, or to be informed before personal data are disclosed for the first time to third parties or used

⁵³ Eleven of 17 submissions supported the proposed right to be removed from a direct marketing list (see submissions L4, L7, L12, L14, L23, S2, S6, S15, S37, S42 and S51). K29 considered that an individual who had authorised the use of information for direct marketing should be entitled later to revoke that authorisation. Four submissions were opposed (L9, L10, L13 and L19) with two suggesting that the issue be addressed by code of practice (L17 and L22).

on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses.

Member states shall take the necessary measures to ensure that data subjects are aware of the existence of the right referred to in the first subparagraph of (b).”

A similar right exists in the Hong Kong privacy law.⁵⁴

- 2.9.15 Given the structure of our information privacy principles I take the view that this proposed new entitlement should be placed in principle 7 with details of any procedural aspects in Part V.



RECOMMENDATION 25

Information privacy principle 7 should be supplemented with a right to prevent the use or disclosure of personal information for the purposes of direct marketing through the deletion or blocking of personal information held by the agency for direct marketing purposes.

- 2.9.16 When a name is taken off a marketing list it should (if practicable) also be taken off lists held by agencies to which the details have been sold or traded. Indeed, complaints will often be made to a user of a list that has been rented from a list broker. It is important that requests to be taken off a list are also notified to the originator. Unless this is done the list information may be used again and again.
- 2.9.17 Existing principle 7(4) and (5) may have to be modified to ensure that renters or purchasers are obliged to notify the requests for deletion to the originator of lists. Principle 3(1)(g) will also oblige agencies which intend to use or disclose information for direct marketing to make the new entitlement under principle 7 known to individuals when collecting personal information from them .
- 2.9.18 I should add that I do not see deletion from mailing lists as being the complete answer to information privacy concerns in relation to direct marketing. If the existing principles were more rigorously applied by agencies the issues would tend to diminish on their own. In particular, agencies should be more open about the collection of personal information where it may be put to direct marketing purposes. The individual should be given an option to agree to this use or at the very least to object to it at the time of collection. Agencies should not portray the secondary use of personal information for marketing purposes as an implicit condition for obtaining goods or services.

2.10 PRINCIPLE 8 - Accuracy, etc, of personal information to be checked before use

- 2.10.1 Under principle 8 an agency must take reasonable care to check that personal information is accurate, up to date, complete, relevant and not misleading, *before* using it. The principle is modelled upon principle 8 in the Australian Privacy Act and is derived from the OECD “data quality principle”. This provides:

“Data quality principle

Personal data should be relevant to the purpose for which they are used, and, to the extent necessary for those purposes, should be accurate, complete and kept up to date.”

- 2.10.2 Principle 8 also ties in with the obligation in principle 7 on an agency, of its

⁵⁴ Personal Data (Privacy) Ordinance 1995 (Hong Kong), section 34.

“Seminar participants are uniformly critical in the approach of the direct marketers.

The Privacy Act should create a right to be removed from a list as this will give people an alternative to proving that the addition of their name to a list was in contravention of any of the information privacy principles or public register privacy principles.”

- KATHRYN DALZIEL,
SUBMISSION S6

own initiative, to ensure the accuracy of information. Principle 7(2) provides:

“An agency that holds personal information shall ... on its own initiative, take such steps (if any) to correct the information, as are in the circumstances, reasonable to ensure that, having regard to the purposes for which the information may lawfully be used, the information is accurate, up to date, complete and not misleading.”

2.10.3 Principle 8 is one of the shorter principles and is, I believe, easily understood. I am satisfied that the principle has worked satisfactorily in operation and this seems to have been borne out in consultation.⁵⁵

Meaning of “use”

2.10.4 In common with principle 10, principle 8 governs the “use” of personal information. There has been some speculation by commentators on the Act as to the meaning of “use” and, in particular, whether:

- the meaning is to be taken as the same as for principle 10;
- it might encompass disclosure;
- browsing information can constitute a use; and
- the process of verifying the accuracy of information itself constitutes use of that information.⁵⁶

2.10.5 On this last point Dr Paul Roth suggests that a way to avoid problems:

“would be to interpret the term ‘use’ in principle 8 in such a way that it does not apply to uses under principle 8 itself. That is, since principle 8 is aimed at the use of personal information without verification, where personal information is disclosed in order to verify its accuracy in compliance with principle 8 such a ‘reflexive’ use ought not to be caught.”⁵⁷

2.10.6 This would seem to be a plausible interpretation which could avoid interpretation difficulties in the utilisation of information for the purpose of verification, whether involving internal agency use or a use also entailing a disclosure.

2.10.7 This leads on to the question of whether an agency must check the accuracy of information when it is simply disclosing the information for use by someone else. The interests of individuals would obviously be harmed if an agency disclosed inaccurate information which was used to the detriment of the individual.

2.10.8 Other principles also bear on this issue in the sense that:

- pursuant to section 7(2) the agency may be obliged, of its own initiative, to take steps to correct information and to ensure that it is accurate having regard to the purposes for which the information may lawfully be used (and this does not appear to be limited solely to the use that the agency itself will make of the information);
- the recipient agency will be obliged in accordance with principle 8 to take such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is proposed to be used, the information is accurate etc.

However, it may be that under principle 7(2) the agency has taken no steps

⁵⁵ Ten out of 13 submissions agreed that principle 8 had worked adequately in operation (submissions K8, K9, K11, K13, K14, K18, K20, K25, K27 and K28). Submissions K12, K19 and K21 had some criticisms of the principle.

⁵⁶ A number of these issues are discussed in *Privacy Law and Practice*, paragraph 1006.42A.

⁵⁷ *Ibid*, paragraph 1006.42A.

as it had not itself contemplated using the information. Also, the recipient agency may have no feasible means to check the accuracy of the information.

- 2.10.9 The disclosure of personal information by an agency for use by someone else is one of the more significant actions that may affect the interests of an individual. Clearly it is undesirable for agencies to recklessly disclose inaccurate personal information without regard to the effect on the individual. It may be that the issue is satisfactorily addressed in our principles. It may be that principle 7(2) as it applies to the agency disclosing the information, and principle 8 as it applies to the recipient agency, together provide an appropriate response. It is also possible that principle 8 might be interpreted in such a way that the action of disclosure (or in a more limited basis the actions preliminary to a disclosure) constitute a “use” for the purpose of principle 8. Certainly there is a school of thought that takes a view that “use” for the purposes of principle 8 does not necessarily exclude the action of “disclosure” as is arguably the case for principle 10 (given that there is a separate disclosure principle 11). There has been no definitive Tribunal or court interpretation on the issue as yet. It may be desirable to make the position plain. A precedent is to be found in principle 3 of the Australian National Principles for the Fair Handling of Personal Information which states:

“An organisation should take reasonable steps to ensure that the personal information it collects, uses or discloses is accurate, complete and up to date.”

- 2.10.10 It may be appropriate to amend our own principle 8 to read as follows:

“An agency that holds personal information shall not use *or disclose* that information without taking such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is proposed to be used, the information is accurate, up to date, complete, relevant, and not misleading.” [change highlighted]



RECOMMENDATION 26

Consideration should be given to amending information privacy principle 8 to substitute the phrase “use or disclose” for “use” in the first line.

2.11 PRINCIPLE 9 - Agency not to keep personal information for longer than necessary

- 2.11.1 Principle 9, which requires that an agency not keep information it holds for longer than is required for the purposes for which that information may lawfully be used, provides support to several of the other principles. The principle discourages agencies from continuing to retain personal information that is no longer needed. A privacy risk exists where such personal data is retained since:
- the information may become out of date and therefore should not be used (see also principle 8);
 - accumulations of personal information create a risk that they will be used regardless of the purpose for which the information was obtained or the ability to approach the individual directly for the same information (see also principles 2 and 11);
 - the retention of personal information well beyond its “use by date” represents an additional and avoidable security risk as it may inadvertently be disclosed (see also principles 5 and 11).

- 2.11.2 The present heading to principle 9 has caused misunderstanding. The princi-

“Principle 8 places an unfair burden on agencies who have been provided with information by a third party with whom the individual has primary contact. The agency that collects the information from the individual should be primarily responsible for ensuring that parties to whom that information is provided are notified of any material changes to the original data eg repayment of an outstanding debt.”

- BAYNET CRA,
SUBMISSION K21

ple does not literally state that an agency is not to keep personal information for “longer than necessary”. Rather, it prohibits keeping information for “longer than is required for the purposes for which the information may lawfully be used.” I have recommended elsewhere that a simple reference to “retention of personal information” in the heading may suffice to avoid confusion.⁵⁸

Other jurisdictions

- 2.11.3 Although a retention principle is not found in all privacy laws, there are similar provisions in several. For example, principle 2(2) of the Hong Kong Personal Data (Privacy) Ordinance states:

“Personal data shall not be kept longer than is necessary for the fulfilment of the purpose (including any directly related purpose) for which the data are or are to be used.”

- 2.11.4 The 1993 Quebec Act Respecting the Protection of Personal Information in the Private Sector (section 12), states:

“Once the object of a file has been achieved, no information contained in it may be used otherwise than with the consent of the person concerned, subject to a time limit prescribed by law or by a retention schedule established by government regulations.”

- 2.11.5 The Australian Privacy Act does not currently have a principle corresponding to principle 9. However, the Australian National Principles for the Fair Handling of Personal Information include as part of a more general data security principle:

“An organisation should take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose”.⁵⁹

- 2.11.6 The UK Data Protection Bill provides at data protection principle 5 that:

“Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.”⁶⁰

Other enactments

- 2.11.7 Principle 9 is subject to the requirements of other enactments. There are, for example, laws requiring taxpayers to retain taxation records and health agencies to retain medical records. In the public sector the Archives Act and Local Government Act require the retention of certain archives.

- 2.11.8 Concerns have occasionally been expressed that over-zealous application of principle 9 might lead to premature destruction of records which may turn out in fact to be useful to the agency or individual and able to be used both lawfully and in accordance with the information privacy principles. The general answer to such a criticism is that the principle does *not* require premature destruction and in such circumstances an agency is able to adopt its own sensible approach to information and document retention. Furthermore, the principle does not oblige the *destruction* of information or documents, but simply obliges the agency no longer to “keep” information. It is possible, for example, for an agency to

⁵⁸ See recommendation 2.

⁵⁹ Australian Privacy Commissioner, *National Principles for the Fair Handling of Personal Information*, February 1998, clause 4.2.

⁶⁰ Data Protection Bill [HL] (UK), introduction version, schedule 1(I).

“Telecom questions the general need for principle 9. However, if it is to be retained then it should not be made more restrictive. Purposes for collection (and retention) of information change over time. It would be unduly restrictive to limit retention to the purposes for which the information was obtained in the first place.”

- TELECOM NEW ZEALAND,
SUBMISSION K12

return documents to the individual concerned or to disclose the information in accordance with principle 11 to an agency that does have a further lawful use for the information. It is possible that the marginal note, already mentioned, contributes to misunderstanding and I have already recommended that that be put right.

2.11.9 In consultation I asked whether principle 9 had led to inappropriate or premature destruction of documents. No evidence was produced of any real or significant problem in that respect. Some submissions speculated that such a risk might exist or asserted that destruction had occurred without giving any specifics. I do not believe that there is a significant problem although I acknowledge the possibility of employees misunderstanding the law and believing that they are obliged to destroy particular documents whereas in fact they are not.

2.11.10 It is possible that, motivated by principle 9, some documents have been destroyed in the last 5 years which were in fact required to be retained under the Archives Act until a disposal schedule had been agreed. If this indeed had happened it is, of course, regrettable but it needs to be understood:

- the actions of destroying such documents would have been based on a *misunderstanding* of the Privacy Act and not the requirements of the law itself;
- the root of any such problem is ignorance of agencies' responsibilities *under the Archives Act* rather than a problem with the Privacy Act.

2.11.11 This latter point raises a particular problem which has arisen in other circumstances as well. The Privacy Act operates as a kind of “overlay” on the actions of public sector agencies which are primarily governed by other legislation. The Act assumes compliance with the requirements of other legislation and, through section 7, provides that the principles defer to the requirements of other enactments. Problems can arise where employees in public sector agencies have not been made aware of agencies' obligations under other statutes. The issue arises not merely in respect of the Archives Act but also with the Official Information Act. The interaction with these pieces of legislation would work more satisfactorily if agencies were more aware of their other statutory obligations. Although the review of the operation of the Privacy Act can identify problems of this sort the solution may be primarily found elsewhere than in the Act or the operations of my Office.⁶¹ In my education and awareness functions in relation to the information privacy principles I do emphasise obligations under other statutes.⁶²

Requirement to retain information

2.11.12 Some people have suggested that individual privacy and personal autonomy can be harmed by premature destruction of personal information as well as its unnecessarily long retention. Examples might include:

- destruction by the sole repository of records concerning a person's origins (such as information about a birth parent in an adoption context or about the donor of gametes in relation to offspring born through assisted human reproduction);
- destruction of records so as to prevent the individual concerned exercising a right of access;
- destruction of records upon which a decision has been based so as to prevent any review of that decision or exercise of any judicial or administrative remedies (for example, records which might have indicated unlawful discrimination in an employment context).

⁶¹ Nonetheless my suggestion for amending section 7 may improve the situation. See paragraph 2.15 and recommendation 31(a).

⁶² For example, my Office released a compilation of materials relating to archiving issues in which the interaction with the Archives Act is canvassed. See Privacy Commissioner, *Compilation of materials in relation to the Privacy Act, Archives and Libraries*, 1995.

“The Department has strong concerns that documents are being destroyed prematurely, in breach of the Archives Act, on the basis that destruction is required by principle 9.”

- DEPARTMENT OF INTERNAL AFFAIRS, SUBMISSION K27

- 2.11.13 In New Zealand, some laws have tried to deal with this issue on a case by case basis. For example, the Health (Retention of Health Information) Regulations 1996 seek to ensure that medical records are retained to be available when needed through the imposition of a ten year minimum retention period. In other contexts, the issue has been addressed by creating statutory registers of certain key details which are always available to be accessed (such as exists with adoption information and has been proposed with respect to assisted human reproduction records).
- 2.11.14 The Freedom of Information and Protection of Privacy Act in British Columbia has tackled this issue directly in respect of the public sector. In a section entitled “Retention of personal information” it states:
- “If a public body uses an individual’s personal information to make a decision that directly affects the individual, the public body must retain that information for at least one year after using it so that the individual has a reasonable opportunity to obtain access to it.”⁶³
- 2.11.15 A provision such as that has characteristics in common with the privacy rights and entitlements contained in information privacy principle 6 and Part V of the Act. It also has something in common with the entitlement that individuals have to obtain access to reasons for decisions affecting a person (a right which is currently found in section 23 of the Official Information Act 1982). That entitlement might well be considered a privacy right or entitlement and indeed it was initially intended to include such a right in the Privacy of Information Bill as an information privacy principle.⁶⁴ This would have replaced the Official Information Act provision. The primary reason for dropping the proposed principle was that its application would be limited to the public sector whereas the Privacy Act was intended to have a generally seamless application to both public and private sectors. That proposed entitlement, and I suggest the obligation to retain information under the British Columbia Act, have as much to do with expectations of procedural fairness in public agencies as with information privacy.
- 2.11.16 It would be problematic to have an obligation of the type in the British Columbia Act apply to all agencies in the public and private sectors. Submissions were almost evenly split on the question of reforming principle 9 to require the retention of information for a minimum period.⁶⁵ If such an obligation were to be applied to public sector agencies solely, I suspect that it would be better to link that obligation to section 23 of the Official Information Act than to the Privacy Act (although the merits either way could be further debated). The Archives Act may well achieve something similar in the public sector anyway.
- 2.11.17 I see the retention of information for minimum periods as a legitimate privacy issue but I suggest that a better way of addressing those concerns than amending principle 9 is through sector specific obligations. An example of this is the Health (Retention of Health Information) Regulations 1996. I have also recommended elsewhere that there should be an offence created where an individual destroys information after an access request is received in order to deny the individual’s entitlement to information (see recommendation 149).
- 2.11.18 To supplement these provisions I suggest that there should be a provision permitting a code of practice to require the retention of certain information or

“Specific minimum periods of retention should be judged on a case by case basis. These should be addressed by legislation or through guidelines dealing with specific issues as they relate to specific sectors. Retention time is not automatically linked to access opportunity. Knowledge of access to a record is a matter of education and information, and not time.”

- CONSUMERS’ INSTITUTE,
SUBMISSION K18

⁶³ Freedom of Information and Protection of Privacy Act 1992 (British Columbia), section 31.

⁶⁴ Privacy of Information Bill, principle 8.

⁶⁵ Eight submissions supported such a change (submissions K8, K11, K19, K20, K25, S24, S36, S42), 8 were opposed (K9, K12, K14, K18, K21, K28, K29, S11) with 3 neutral (K10, K13, K27).

documents. The requirement would be predicated on the possibility of individuals exercising their rights under the Act rather than directed towards any need by society for long term retention of documentation. Accordingly, I suggest that the power be limited to require the retention of information for a period not exceeding six years (which corresponds with the limitation period under the Limitation Act in most cases). The code making power would not be intended to be used to require long term records to be held on such matters as adoption or assisted human reproduction.



RECOMMENDATION 27

Section 46(4) should be amended to provide that a code of practice may require an agency to retain specified information or documents for a specified period, not exceeding six years.

2.12 PRINCIPLE 10 - Limits on use of personal information

2.12.1 Principles 10 and 11 give effect to the OECD “purpose specification principle” and “use limitation principle”. Limiting use and disclosure of personal information other than for purposes specified at the time of collection (or compatible purposes or those authorised by the individual concerned or by law) lies at the heart of any data protection law.

2.12.2 Principle 10 itself is straightforward and runs only to a single sentence. However, the detail is to be found in the list of 12 exceptions. Although principle 10 is an important, and central, principle I have no recommendations for amendment at this time. It appears to have worked satisfactorily albeit that there is often room for dispute as to precisely the purpose or purposes for which information was obtained.

Exceptions

2.12.3 Thirteen submissions responded to a question in the discussion paper asking whether the current exceptions to principle 10 are satisfactory or should be amended or any of them omitted. The submissions were almost equally split with seven submissions suggesting that the current exceptions are satisfactory⁶⁶ and six urging amendment.⁶⁷ No single pattern emerged from the submissions urging change although several did mention the individual authorisation exception as warranting amendments for example:

- to be more specific, for example requiring authorisation for a specific purpose;
- to be documented by being in writing;
- to spell out the elements of authorisation, for example being “free and informed consent”;
- to enable an individual to withdraw authorisation, for example by being taken off a mailing list.

2.12.4 Principles 2, 3, 10 and 11 presently include an exception where the individual concerned “authorises” the collection, use or disclosure of information by the agency. In recommendation 20 I propose that the individual authorisation exception be dropped from principle 3.

2.12.5 A key issue with such exceptions is whether the individual must positively indicate agreement to the departure from a principle or whether authorisation can be inferred from the circumstances. Commentators have suggested that the concept of authorisation is stronger than that of consent with the verb “authorise” more clearly denoting a positive and conscious act by the individual compared with “consent” where an act is being performed by another in relation to

⁶⁶ Submissions K14, K15, K19, K22, K25, K28 and K29.

⁶⁷ See submissions K11-K13, K18, K21 and F11.



“Exception (b) needs to be more specific, particularly to require authorisation for that other purpose specifically and in writing with free and informed consent with the onus being on the user to demonstrate the consent is free and informed.”

- AUCKLAND DISTRICT

COUNCIL OF SOCIAL SERVICE,

SUBMISSION K1.1

the individual concerned, who is in a passive position. On a complaint I have expressed my opinion that authorisation requires a positive act.⁶⁸

- 2.12.6 Even where a positive action is taken to give authorisation there sometimes remains a problem of specificity. Some agencies ask customers to sign authorisations, unlimited in time and subject matter, essentially purporting to authorise the agency to collect anything from anyone at any time and to use and disclose the information for any purpose to any person. Some might see this as attempting to contract out of some of the limitations imposed by the information privacy principles. Others may see collection of personal information by such means as “unfair” and in breach of principle 4.
- 2.12.7 All privacy laws have grappled with these issues. For example, article 7(a) of the EU Directive on Data Protection provides that personal data may be processed if the individual concerned “has unambiguously given his consent”. The Quebec Act Respecting the Protection of Personal Information in the Private Sector 1993 states in section 15 that:

“Consent to the communication or use of personal information must be manifest, free, and enlightened, and must be given for specific purposes. Such consent is valid only for the length of time needed to achieve the purposes for which it was requested.

“Consent given otherwise than in accordance with the first paragraph is without effect.”

- 2.12.8 In my view, the requirement for “authorisation” in the relevant exceptions to our principles is of similar effect to the concepts elaborated upon in Europe and Quebec. In the absence of any Tribunal or court decision suggesting otherwise I do not see the need to amend the Act to so provide. In terms of the submission suggesting that persons should be able to revoke an earlier authorisation enabling details to be used for direct marketing, I have made a proposal in respect of principle 7 to address this issue.⁶⁹ I have also canvassed the issue of “browsing”, which is relevant to principle 10, in the context of a proposal for defining the term “use”.⁷⁰

2.13 PRINCIPLE 11 - Limits on disclosure of personal information

- 2.13.1 Principle 11 gives effect to the OECD “purpose specification” and “use limitation” principles. Although some overseas laws combine the notion of use and disclosure into a single principle the New Zealand Act has discrete use and disclosure principles.
- 2.13.2 As with principle 10, the main point of discussion in respect of principle 11 concerns its exceptions rather than the basic principle of non-disclosure itself. Some aspects of principle 11 are explicitly or implicitly discussed elsewhere in this chapter, for example:
- the issues of individual “authorisation” arise in respect of principle 11 at least as much as with principle 10;
 - the direct marketing issues mentioned in respect of principle 7 and 10 are also issues under principle 11;
 - the saving of the effect of other statutes which authorise or require information to be disclosed is discussed in some detail in relation to section 7.⁷¹

⁶⁸ See case note 2976.

⁶⁹ See recommendation 25.

⁷⁰ See recommendation 16.

⁷¹ The requirements relating to section 7 are discussed at paragraph 2.15.

“In respect of the word ‘authorised’, implied authority in respect of the use of the personal information should be acceptable.”

- BAYNET CRA LIMITED,
SUBMISSION K21

- 2.13.3 On this last point, it would be fair to say that some people have been confused as to the extent to which agencies can refuse to release information requested under the Official Information Act in reliance on principle 11. The position briefly stated is that if another enactment authorises or requires information to be disclosed this will prevail over principle 11 - see section 7(1). The Official Information Act is an enactment which may authorise or require information to be disclosed and therefore such requests should be dealt with in terms of that other statute rather than principle 11 (although, in appropriate cases, personal information may be withheld under that Act where necessary to protect the privacy of natural persons). My recommendation to transfer the substance of section 7(1) into principle 11 itself will, I believe, diminish misunderstanding on this score.⁷²
- 2.13.4 The discussion paper asked whether any of the exceptions to principle 11 should be amended or omitted. Twenty submissions were received with 13 suggesting amendment⁷³ and 7 submitting that the exceptions should be left alone.⁷⁴
- 2.13.5 There was no clear theme emerging from submissions advocating amendment. A number simply referred to their suggestions in respect of the exceptions to principle 10, particularly with respect to individual authorisation. One or two submissions expressly addressed matters that are dealt with in the Health Information Privacy Code 1994 which are therefore not particularly relevant to this exercise.

Disclosure for enforcement of foreign laws

- 2.13.6 The discussion paper also asked whether any new exceptions should be inserted into principle 11. Few submissions were received on this question with seven of the 12 submissions opposing the inclusion of new exceptions.⁷⁵ Five submissions advocated new exceptions.⁷⁶ Two of those submissions suggested that a new exception ought to be provided to enable the disclosure of information to law enforcement authorities to enable the maintenance of *overseas* laws.⁷⁷ This was in fact posed as a separate question which drew considerable support with eight submissions supporting the creation of such an exception,⁷⁸ two submissions opposing it⁷⁹ and three others offering observations.⁸⁰
- 2.13.7 The reason for raising the question of disclosure to overseas law enforcement agencies, is that the present exception provided in paragraph (e) in relation to the maintenance of the law is probably unavailable for such disclosures since it is linked to the notion of avoiding prejudice to the maintenance of the law by any “public sector agency” (which means a *New Zealand* public sector agency). This is likely to mean that the prejudice to the law covered may only be in relation to a *New Zealand* law. Accordingly, it is arguable that if disclosure is not otherwise permitted by principle 11, disclosures to overseas agencies to enable the investigation or prosecution of a foreign offence would only be permissible under the provisions of another enactment (such as the Mutual Assistance in Criminal Matters Act 1992).

- 2.13.8 Partly as a response to this issue, a specific provision was included in the Customs and Excise Act 1996. This permits the disclosure of certain specified

⁷² See recommendation 30.

⁷³ See submissions K7, K10-K13, K17-K19, K21, K29, S11, S19 and S25.

⁷⁴ See submissions K9, K14, K22, K23, K27, K28 and S13.

⁷⁵ See submissions K11, K13, K14, K18, K22, K23 and K28.

⁷⁶ See submissions K12, K19, K21, S11 and S15.

⁷⁷ See submissions K12 and S11.

⁷⁸ See submissions K3, K10-K13, K18, K21 and S11.

⁷⁹ See submissions K25 and S42.

⁸⁰ See submissions K19, K20 and K28.

“After some initial confusion, there have been few problems experienced by member services which can be traced to the Act itself. Difficulties appear mainly to stem from misapplication of the Act by those attempting to use it, or in some cases to hide behind it. This may suggest a need for greater emphasis on community education. The privacy principles have so far proved sound and realistic. Accessing training in the application of the Act has represented a considerable compliance burden for community organisations such as ours.”

- NZ FEDERATION OF FAMILY
BUDGETING SERVICES,
SUBMISSION S29

information from the NZ Customs Service to overseas customs organisations for certain defined purposes so long as the disclosure is pursuant to an agreement between the two customs organisations.⁸¹

- 2.13.9 In the discussion paper it was noted that the Nova Scotia Freedom of Information and Protection of Privacy Act 1993 might suggest a model if a new exception were to be warranted. That Act permits the disclosure of personal information:

“If the public body is a law enforcement agency and the information is disclosed ... to a law enforcement agency in a foreign country under an arrangement, written agreement, treaty or legislative authority.”⁸²

- 2.13.10 While there was support in the submissions for such a proposal there was also concern expressed that any such exception should be tightly controlled.⁸³ It was also suggested that it might be appropriate to limit the foreign agencies/countries to which it applies.⁸⁴ However, there was no submission from any affected law enforcement agency suggesting that there was a real problem to be addressed. None claimed that the principle was too restrictive or that the lack of other legislative authority for disclosure presented a problem for the maintenance of the law or cooperation with other law enforcement agencies. Indeed, the Ministry of Justice, the only core justice agency to make a submission on this question, did not unequivocally support such an exception but rather queried whether there was evidence of it being necessary. Mindful of the sensitivities surrounding enforcement information, and the exhortation in the OECD guidelines that exceptions to the principles should be “as few as possible” I am not inclined to recommend a new exception at this time. The matter could be reconsidered in the future if evidence of a problem emerges.

2.14 PRINCIPLE 12 - Unique identifiers

- 2.14.1 Principle 12 has some characteristics that set it apart from the other principles. For example, it does not mention “personal information” (although the definition of “unique identifier” refers to individuals and the identifier would constitute “personal information”). It also appears more prescriptive than some of the principles. This may have arisen by reason of the fact that the controls were not originally devised as a principle but as a clause in the original bill.⁸⁵

- 2.14.2 Although there is no direct equivalent of principle 12 in the OECD guidelines, other privacy laws and legislation place restrictions in relation to unique identifiers. For example, Australian and American privacy legislation place tight controls on the use of the tax file number⁸⁶ and Social Security Number.⁸⁷ The new UK Data Protection Bill proposes to allow the Secretary of State to prescribe special conditions in relation to any “general identifier”.⁸⁸ Controls on the use of the Identity Card Number and other personal identifiers have been imposed by code of practice under the Hong Kong privacy law.⁸⁹

⁸¹ Customs and Excise Act 1996, section 281. The provision requires consultation with the Privacy Commissioner.

⁸² Freedom of Information and Protection of Privacy Act 1993 (Nova Scotia), section 27(m)(ii). There would be no need, in the present New Zealand Act, to refer to “legislative authority” since this is already encompassed in section 7(1).

⁸³ See, for example, submissions K11, K13 and K18.

⁸⁴ See, for example, submission K13 and K19.

⁸⁵ Privacy of Information Bill, clause 108.

⁸⁶ Privacy Act 1988 (Australia), section 17 and Tax File Number Guidelines.

⁸⁷ Privacy Act 1974, USA, section 7.

⁸⁸ Data Protection Bill [HL] (UK), introduction version, Schedule 1, Part II, clause 4.

⁸⁹ Privacy Commissioner for Personal Data, *Code of Practice on the Identity Card Number and other Personal Identifiers*, Hong Kong, December 1997.

2.14.3 Principle 12 has taken a broad approach in seeking to address all unique identifiers, not simply specifically identified numbers. Principle 12 may thereby have the potential to be more effective than some overseas controls limited to a single identifier. Conversely, the principle's broad coverage may have extended its reach beyond the prime area of concern and may have caused unnecessary compliance difficulties.

2.14.4 Principle 12 has four parts to it. While having a degree of inter-relationship they each impose separate specific requirements, perhaps contributing to the perceived complexity of the principle - other principles tend to impose just a single requirement, or a couple of requirements, albeit sometimes accompanied by a series of exceptions of varying complexity. In fact, taken individually, the parts of principle 12 are relatively straightforward to understand and apply. Nonetheless, principle 12 appears to be the least well understood of the principles with many users of the Act perplexed as to its purpose and effect.

Rationale for principle 12

2.14.5 It is difficult to briefly encapsulate the underlying purposes of principle 12 in the way that one can for the other principles. Instead, there are a variety of concerns to which principle 12 is intended as a response. Dr Paul Roth has attempted to articulate the rationale for principle 12 in *Privacy Law and Practice*. He identifies the following features which I summarise:

- Principle 12 is in response to concerns about the accuracy and use of personal information where a unique identifier is assigned. In particular, the risk is that if one unique identifier is used for a wide variety of authentication and identification purposes in both the public and private sectors this would amount to a de facto universal identifier. De facto universal identifiers have been viewed as unsatisfactory because they are unreliable and a threat to individual privacy.
- Because a de facto universal identifier is not designed to be a true universal identifier it can be technically unreliable and vulnerable to falsification or error.
- Any unique identifier that facilitates the exchange and matching of personal information held by different agencies and within different record systems is perceived to be a threat to privacy. This may also lead to the socially undesirable practice of compiling composite profiles of individuals which may lead to any and every aspect of their lives being open to potential scrutiny by governments or private enterprise.
- The fear is that a de facto universal identifier emerging could ease the way towards the requirement of a national identity card or document. This brings with it a variety of concerns about inaccuracies and such like and the constraint on liberties. For some the idea of a national identity card is equated with the mechanisms of a Police State where identification can only be authenticated and entitlements made upon presentation of the card. Loss, lack or confiscation of such a card makes the individual a “non-person”.⁹⁰

2.14.6 Dr Roth concludes his characterisation of the rationale of principle 12 as follows:

“Accordingly, principle 12 is intended to promote data quality and impose an important form of control on the transfer and linking of individuals’ personal information. Principle 12(1) is intended to control the use of unique identifiers and define when it would be legitimate for an agency to assign them. Principle 12(2) controls the re-assignment of unique identifiers and thereby aids in promoting data quality and discourages illegitimate profiling and

⁹⁰ *Privacy Law and Practice*, paragraph 1006.65.

data matching of individuals. Principle 12(3) is directly concerned with data quality in that agencies must take all reasonable steps to verify the identity of individuals who are assigned unique identifiers. Finally, principle 12(4) controls the use of unique identifiers by restricting their use to the purposes in connection with which they were assigned, or a directly related purpose, and by requiring agencies not to require disclosure otherwise of unique identifiers. This is intended to discourage the illegitimate use of unique identifiers and their collection for linking or profiling purposes. It also individually promotes data quality, since restricting the spread of individuals' unique identifiers makes it less likely that incorrect, inaccurate or outdated personal information will later be used.”⁹¹

- 2.14.7 In addition to the points made by Dr Roth it might also be noted that:
- information matching rule 2 supplements principle 12 by prohibiting the use of unique identifiers in authorised information matching programmes except as provided in another enactment;
 - principle 12 inter-relates with the other eleven information privacy principles in so far as a unique identifier will be “personal information” and subject to the other principles;
 - the controls in principle 12 can supplement the objectives of various of the other principles, for example, principle 12(3) goes to the reliability of information, a matter also of concern in principle 8, while principle 12(4) touches upon the purposes for collection and disclosure of information, relevant to principles 1 and 11;
 - some individuals hold religious concerns about the process of numbering individuals. Others see the process as dehumanising (with the tattooing of concentration camp inmates as the most extreme example).

The meaning of “assign”

- 2.14.8 Each of the four clauses in principle 12 uses the term “assign”. That term is not defined in the Act and has sometimes caused confusion. The *Concise Oxford Dictionary* defines it as “ascribe or refer to”. However, it would not make the meaning any plainer to substitute “ascribe” for “assign”.
- 2.14.9 I have given consideration to including in the Act a definition of “assign”. Although the matter was raised in consultation no suitable definition has been suggested. I have concluded that it may instead be preferable to rely upon its ordinary English meaning and allow the meaning to be clarified over time in real cases. So far, there have been very few principle 12 complaints by which its meaning could be clarified and tested against real sets of circumstances. Most submissions did not favour attempting to define the term.⁹²
- 2.14.10 There are two main contexts in which agencies become confused as to whether an identifier has been “assigned”. The first is where the agency simply records the number on its files for later use but does not utilise the number to refer to the individual. An example is a bank which records the tax file number of an individual on the customer’s file. The number is not used for the bank’s own purposes in identifying the individual - it will have its own unique bank customer number - but for taxation purposes and to enable tax certificates to be printed which bear the identifier. In my view, this sort of arrangement will not generally constitute assignment since the number in the bank’s hands, in that scenario, probably does not even constitute a “unique identifier” (the defini-

“The Commission does not believe that the term ‘assign’ should be defined in the statute as it has a common meaning which is quite sufficient for the purpose of the Act.”

- STATE SERVICES COMMISSION,
SUBMISSION S11

⁹¹ *Ibid*, paragraph 1006.65.

⁹² See submissions K14, K19, K25, K28, S11 and S42. Submissions K11, K12 and K22 wished to see the term defined.

tion of unique identifier in section 2 requires the identifier to uniquely identify the individual in relation to the agency). Unless the bank has structured its data such that on being presented with the tax file number it can identify the customer in its records it has likely not assigned a unique identifier.

- 2.14.11 The second context for confusion is where there is a process for the generation of a set of numbers by a central agency which are allocated, often in batches, to agencies which may then utilise those numbers. The allocation process ensures that a particular number does not become available for allocation except on a single occasion. Such a process exists in relation to, say, the National Health Index (NHI) number in the health sector or the Law Enforcement Agency Reference Number (LEARN) in the justice sector. In my view, the mere generation of numbers is not sufficient to constitute assignment. Rather the identifiers need to be brought into effect in an agency for the purposes of uniquely identifying particular individuals. However, that has yet to be tested in a real complaint or Tribunal proceedings.

Limiting principle 12(2) to public sector unique identifiers

- 2.14.12 It may be argued that principle 12(2) goes further than necessary to meet reasonable privacy objectives and therefore possibly unduly causes compliance difficulties.
- 2.14.13 I consider that it is possible to limit the scope of principle 12(2) while still addressing the primary privacy concerns. Any increased privacy risk which might follow from cutting back its coverage can be compensated by a power to reassert the prohibition in particular circumstances by code of practice. The change would contribute to reducing compliance costs.
- 2.14.14 I consider that principle 12(2) could safely be limited to unique identifiers that are originally generated, created or assigned, by or on behalf of public sector agencies. If that change were to be made then both private and public sector agencies would continue to be prohibited from reassigning an unique identifier where the agency knows that the number had been assigned to an individual by a public sector agency. This would, for example, continue the prohibition on utilising the tax file number as a unique identifier but would mean that, for example, the problem which led to the Superannuation Scheme Unique Identifier Code 1995 would not arise.⁹³

- 2.14.15 Essentially this is what has been proposed in the Australian Privacy Commissioner’s National Principles for the Fair Handling of Personal Information. The Australian Privacy Act does not currently have a principle dealing with the assignment of unique identifiers but there has been a strong concern, particularly following the “Australia Card” debate, about the use of the tax file number. The proposed new principles are intended as suitable for the private sector and include the following principle on identifiers:

“7.1 An organisation should not adopt as its own identifier an identifier that has been assigned by a government agency (or by an agent of, or contractor to, a government agency acting in its capacity as an agent or contractor).

7.2 An organisation should not use or disclose an identifier assigned to an individual by a government agency (or by an agent of, or contractor to a government agency acting in its capacity as agent or contractor) unless one of paragraphs 2.1(d) to 2.1(h) applies.”

- 2.14.16 While there are no current “private” national unique identifiers it is conceiv-

⁹³ The Superannuation Schemes Unique Identifier Code 1995 could be revoked if this proposal is adopted.

“The Federation is of the view that rather than an attempt to define the word ‘assign’, it would be better for an advice booklet to give examples of ways in which the word is intended to apply. A definition would be unlikely to provide complete clarity.”

- NZ EMPLOYERS

FEDERATION, SUBMISSION K1.4

able that one might be devised, or arise through common usage. For example, there has been speculation that in the future individuals could be assigned with telephone numbers which they would carry throughout their lives. That in itself would not necessarily be a problem under principle 12(2) but if a wide range of agencies were to adopt the same number to identify the individual there would be an issue. This may be addressed by the Commissioner reimposing principle 12(2), in modified or unmodified form, to an identifier assigned by a private sector agency by way of code of practice.

- 2.14.17 There was little support in submissions for the proposal that principle 12(2) should be limited so that the prohibition is solely on the reassignment of numbers originally generated, created or assigned by a public sector agency.⁹⁴ Nonetheless, I consider the proposal is worthwhile.



RECOMMENDATION 28

In relation to the controls on reassignment of unique identifiers:

- (a) information privacy principle 12(2) should be limited so that the prohibition is solely in relation to the reassignment of unique identifiers originally generated, created or assigned by a public sector agency; and**
- (b) section 46(4) should be amended to make it clear that a code of practice may apply the controls in principle 12(2) to the assignment of unique identifiers generated, created or assigned by any agency (not simply a public sector agency).**

Enforceability of principle 12(2)

- 2.14.18 When the Privacy of Information Bill was introduced it provided for the making of regulations governing the creation and use of unique identifiers. The regulations would have prescribed offences carrying a maximum \$10,000 fine. The proposed provision was replaced by principle 12.
- 2.14.19 Principle 12(1), (3) and (4) are traditional data protection provisions for which the normal complaint and remedy process, focusing upon an individual's circumstances and the harm to that individual, fit satisfactorily. For example, it is conceivable that a complaint might be received and satisfactorily processed in the following circumstances:
- principle 12(3) - an agency fails to take all reasonable steps to ensure that unique identifiers are assigned to individuals whose identity is clearly established and as a result takes actions against a wrong individual;
 - principle 12(4) - an agency denies goods or services to an individual who refuses to supply a unique identifier in circumstances where the identifier should not have been demanded.
- 2.14.20 However, the complaints and enforcement procedures are unlikely to be effective in relation to the re-assignment provision in principle 12(2). In particular:
- re-assignment is likely to be done on a system-wide basis rather than on the individual basis upon which complaints normally arise;
 - it will often be difficult to show any particular harm or detriment for the action of re-assignment so as to constitute an "interference with the privacy of an individual" under section 66(1)(b). However, the re-assignment may be the key to future information sharing in breach of principles 2, 10 or 11, which cannot be proved (and may not even have been intended) at the time of re-assignment.
- 2.14.21 In consultation I asked whether the enforcement of principle 12(2) should be enhanced. Not many responses were received partly, I suspect, because many users of the Act find principle 12 perplexing or have had no real experience

"It is unlikely that actions of private sector agencies would create a common national identification number. If that situation did arise the Commissioner could address it by reintroducing a restriction through a code of practice."

- ASSOCIATION OF SUPERANNUATION FUNDS OF NEW ZEALAND, SUBMISSION K24

⁹⁴ Submissions K13 and K24 agreed with the proposal while 5 submissions disagreed - K11, K14, K18, K19 and K28. Other comments were received in submissions K12, S36 and S42.

with it. The responses were approximately evenly split with five submissions favouring an enhancement of the enforceability of principle 12(2)⁹⁵ with four opposed.⁹⁶

- 2.14.22 With the proposed limitation of principle 12(2) to identifiers assigned by public sector agencies it may well be appropriate to revert to an offence provision, the mechanism originally proposed in the bill. However, I am reluctant to depart from the civil law approach which underpins the Privacy Act's enforcement of the information privacy principles. I consider a preferable alternative to be modification of section 66 so as to remove the present harm or detriment requirement in relation to certain types of complaints involving principle 12(2).
- 2.14.23 I propose that individual complaints of a breach of principle 12(2) should continue to have to satisfy the existing requirements of section 66(1)(b) to constitute an "interference with the privacy of an individual" but that in certain circumstances proceedings be available for breach without having to prove harm or detriment of the type listed in section 66(1)(b). The circumstances I have in mind are where the re-assignment is "wilful" by which I mean cases for which compulsion or ignorance or accident cannot be pleaded as an excuse. The actions to be covered are those in which the assignment is intentional and deliberate notwithstanding the agency's awareness of the prohibition in principle 12(2). Such actions will almost certainly involve a continuing or on-going practice of assignment in breach of the principle. While damages could not be awarded, an order could be made by the Complaints Review Tribunal in relation to continuing or repeating the interference.



RECOMMENDATION 29

Section 66(1) should be amended so that an interference with privacy may be established notwithstanding the absence of any harm or detriment of the type set out at section 66(1)(b) in cases of wilful breach of information privacy principle 12(2).

2.15 SECTION 7 - Savings provision

- 2.15.1 Section 7 is a savings provision. In effect, it provides that the Privacy Act is subject to the provisions of any other enactment (which includes regulations) dealing with a matter which would otherwise be determined solely by reference to the information privacy principles. Moreover, an action will not constitute a breach of principles 1-5, 7-10 and 12 if that action is authorised or required by or under law. Section 7 essentially recognises specific public interests contained in a variety of other enactments and provides for their continuation, and recognition, under the Privacy Act.
- 2.15.2 While there might have been some benefit in having a Privacy Act which did override other legislation in terms of certainty of the rules in relation to personal information, there would have been considerable, and understandable, opposition from those organisations already applying their own regime under specific legislation. Much research would have been required to identify all legislation which might include provisions covering information issues of the time the Privacy Act was passed. Parliament decided to meddle with existing legislation as little as possible.
- 2.15.3 It may be acknowledged here that international human rights treaties allow rights to be limited so long as the limits are set out in law. This provides for certainty and transparency. It also permits limited and justified departures from the expected rights, when made democratically.

⁹⁵ See submissions K11, K13, K19, K21 and S11.

⁹⁶ See submissions K14, K18, K23 and K28.

2.15.4 By way of contrast with the New Zealand position it may be of interest to know that many Canadian provinces have provisions in their privacy legislation which provide that their privacy law will override a subsequent general Act unless the latter Act is expressly provided to prevail notwithstanding the privacy legislation.⁹⁷

Subsections 7(1) to (6)

2.15.5 Section 7 is a key, but rather complicated, provision which essentially provides that all other legislation (both statutes and regulations) will override the principles identified in the various subsections on specified matters. It is particularly unusual to allow regulations to override an Act. The normal rule would be that Acts have priority over regulations.

2.15.6 Section 7(1) provides that a specific provision in another *enactment* (that is, act or regulation) authorising or requiring personal information to be made available will override principles 6 (access to personal information) and 11 (limits on disclosure of personal information).

2.15.7 Section 7(2) provides that a specific provision in any *Act* prohibiting or restricting the availability of personal information, or regulating the way in which personal information may be obtained or made available, will override principles 6 and 11.

2.15.8 Section 7(3) applies the same regime as subsection (2) to provisions in *regulations*⁹⁸ but complicates the situation by limiting its application to regulations in force before the Official Information Act was passed in relation to the public sector, regulations in force before the Local Government Official Information and Meetings Act was passed in relation to local authorities, and regulations in force before the Privacy Act was passed in relation to any other agencies.

2.15.9 Section 7(4) provides that an action done will not be a breach of any other of the principles other than principles 6 and 11 if that action is authorised by “or under law”.

2.15.10 Section 7(5) provides that nothing in principle 7, which concerns correction of personal information, applies in respect of any information held by the Department of Statistics where that information was obtained pursuant to the Statistics Act 1975.

2.15.11 Finally, section 7(6) provides, subject to the provisions of Part VII, nothing in any of the information privacy principles is to apply in respect of a public register. This provision is discussed in relation to section 60 where a recommendation for reform is made.⁹⁹

Simplifying the savings regime

2.15.12 The existence of section 7 is critical to understanding the present regime for the interaction between the information privacy principles and other laws. Unfortunately, ignorance concerning its existence and effect has sometimes led to

⁹⁷ See, for example: An Act Respecting the Protection of Personal Information in the Private Sector, 1993 (Quebec), section 94; An Act Respecting Access to Documents held by Public Bodies and the Protection of Personal Information 1982, (Quebec), sections 168 and 169; Freedom of Information and Protection of Privacy Act 1992 (British Columbia), section 78. The British Columbia Act provides that “if a provision of this Act is inconsistent or in conflict with a provision of another Act, the provision of this Act prevails unless the other Act expressly provides that it, or a provision of it, applies despite the fact”.

⁹⁸ Only regulations made by Order in Council are covered. A problem has arisen in respect of the Status of Financial Reporting Standards which are regulations for the purpose of the Regulations (Disallowance) Act but are not issued by Order in Council.

⁹⁹ See paragraphs 7.8.1 - 7.8.15 and recommendation 92.

difficulties in the operation of the legislation. The typical problem involves an agency which believes that it is unable to utilise information in a particular way because it is not permitted by an information privacy principle. Such agencies are sometimes unaware, or purport to be unaware, that the action may well be permitted by other legislation which authorises or requires it.

2.15.13 If one accepts the basic proposition that the information privacy principles should be overridden by other specific laws, as I do, then section 7 can probably be seen technically as a satisfactory and effective provision. Unfortunately, the provision cannot be fully effective unless its content is known to the persons who must apply the principles, particularly agencies which hold information which is subject to other laws. My suggestions for improving the position in that regard involve:

- a new marginal note;
- dispersal, where appropriate, of some elements of section 7 into the relevant information privacy principles;
- simplification of section 7.

I also make some suggestions for modest substantive changes to section 7 to enhance privacy rights while simplifying the position at the same time.

Marginal note

2.15.14 I have recommended elsewhere that the marginal note should be made more informative given that many people working with the Act are not familiar with technical statutory terms such as “savings”.¹⁰⁰ I suggest that the marginal note should be altered from “Savings” to “Saving of effect of other laws” or “Effect of other laws on information privacy principles”.

Dispersal of elements of section 7

2.15.15 Persons who frequently use the Privacy Act realise the importance of section 7 and generally do not have too many difficulties with it. However, less familiar users, particularly those who have a copy of the information privacy principles but not the other parts of the Act, are sometimes unaware that the principles are not the last word on the subject of collection, use and disclosure of personal information, and must be read subject to other enactments. This is not apparent from reading the principles themselves. It is necessary to read section 7. People unaware of section 7 have sometimes wrongly suggested that the principles fail to acknowledge public interests which compete with privacy. I suggest that parts of section 7 be dispersed to form part of the principles to which they relate. On this basis agencies and their staff will have a better picture of the effect of the principle when reading the principle alone.

2.15.16 There is a downside to dispersing elements of section 7 into the principles. In particular the principles will expand in length. It is fair to say that section 7 was adopted as a mechanism to avoid cluttering the various principles with repeated lengthy exceptions saving the effect of other laws. However, I think the proposal for dispersal need only modestly increase the length of the principles.

2.15.17 My proposal for dispersal of sections 7(1), 7(4) and 7(5) involves transferring elements of the following subsections into the relevant principles:

- section 7(1) - transfer into principle 11 (the aspect concerning principle 11 only);¹⁰¹
- section 7(4) to be transferred into principles 1 to 5, 7 to 10 and 12;
- section 7(5) which relates to a single law and a particular agency, should not be transferred into a principle but should instead remain in section 7 or be placed with the exemptions in Part VI.

¹⁰⁰ See recommendation 2.

¹⁰¹ The aspect of section 7(1) concerning principle 6 may remain where it is.

2.15.18 In the context of section 7(1), the official information statutes are the main enactments which authorise or require personal information to be made available. They also seem to be the statutes most overlooked by public sector staff receiving a third party request for someone’s personal information. A number of submissions considered that section 7 should make clear how the effect of the Official Information Act is saved.¹⁰² Accordingly, in transferring the elements of section 7(1) into principle 11 thought should be given to referring to those statutes. Indeed, this was the approach taken in the disclosure principle in the Privacy of Information Bill which contained an exception relating to where:

The disclosure is made pursuant to any provision of the Official Information Act 1982 or the Local Government Official Information and Meetings Act 1987.¹⁰³

2.15.19 The select committee dropped the exception and, in effect, incorporated it into the more general savings provision, section 7(1). While the legal effect is the same, the experience of the last five years suggests that public understanding might have been enhanced by remaining with the original drafting. If the exception were to be reinstated it could, instead of simply mirroring section 7(1), provide something along the lines of the following:

That the disclosure is made pursuant to a provision of the Official Information Act 1982, the Local Government Official Information and Meetings Act 1987 or any other enactment that authorises or requires personal information to be made available.¹⁰⁴

This will strengthen knowledge of the Official Information Act and Local Government Official Information and Meetings Act which is not well understood by all public sector employees.



RECOMMENDATION 30

Section 7(1) should be amended by transferring its content, in so far as it relates to information privacy principle 11, into principle 11 as a new exception.



RECOMMENDATION 31

Consideration should be given to transferring the content of:

- (a) section 7(4) into information privacy principles 1 to 5, 7 to 10, and 12 as exceptions; and**
- (b) section 7(5) into Part VI.**

2.15.20 Several provisions in section 7 touch upon the access rights arising from information privacy principle 6. The place where users of the Act will expect to see provisions allowing for withholding information is Part IV which sets out the good reasons for refusing access to information.¹⁰⁵ Accordingly, the content of section 7(2) and 7(3), in so far as they relate to principle 6, should be transferred into a new section to appear in Part IV, perhaps as section 29A.

2.15.21 This was the approach that was taken in the Privacy of Information Bill prior to

¹⁰² See submissions M1, M4, M7, M10, M13, M17, S1, S19, S20, S31 and S42. Submissions M8, M16 and S11 saw no need for change in this regard.

¹⁰³ Privacy of Information Bill, principle 14(1)(d).

¹⁰⁴ A similar approach could be taken to the transfer of elements of section 8(4) into principle 9 by making special reference to the Archives Act.

¹⁰⁵ Although some aspects of these subsections might be said to belong in Part V (such as section 72(2)(b)), it will be simpler to place all the material in Part IV.

“The effective interaction of the Official Information Act and the Privacy Act is crucial in terms of day to day access to information held by the public sector. We are aware of requests for information being made of Government departments which are refused on the grounds of the Privacy Act meaning the journalist concerned has to make the request again under the Official Information Act. Clearly Government officials are unsure of the boundary between the two statutes.”

- COMMONWEALTH PRESS UNION
SUBMISSION M13

the select committee’s decision to bring all the savings provisions affecting the information privacy principles together into section 7.¹⁰⁶ I believe that it will make more sense for people who must work with the Act, and apply it to requests for information, to have this provision located in Part IV, to which reference is expressly made in principle 6, than in section 7. Indeed, to treat the provision very much like the other reasons for refusal set out adjacent to section 29 will somewhat dispel the fiction perpetrated by section 30 that refusal is not permitted for any other reason than those set out in sections 27 to 29. If this proposal is adopted a resultant amendment will also need to be made to section 30.



RECOMMENDATION 32

The content of section 7(2) and (3), in so far as they relate to information privacy principle 6, should be relocated into Part IV.

Sections 7(2) and (3) as they concern principle 11

- 2.15.22 Principle 11 prohibits the disclosure of personal information subject to exceptions. It is not a principle which actually authorises the release of information which is otherwise prohibited or restricted. Nor does principle 11 have anything to say about the manner in which personal information may be obtained or made available. It might therefore seem that if subsections (2) and (3) omitted any mention of principle 11 there might be no change in effect - one might continue to say that principle 11 did not derogate from any Act or regulation which does the things specified in those subsections.
- 2.15.23 It has been suggested that the reference is included merely out of caution so as to ensure that there is no misunderstanding on the point. Supporters of this view would suggest that the reference to principle 11 is intended to give comfort to agencies which hold information which may be subject to other enactments that those laws continue to have effect. If that is the sole objective I believe that it has been rather confused by unnecessarily combining the provision with principle 6.
- 2.15.24 The position would become clearer if the principle 11 and principle 6 provisions were to be disentangled. This will occur if my recommendation is accepted to transfer the content of the section 7(2) and (3), in so far as they relate to principle 6, into Part IV of the Act. However, even if that material is not relocated, there will still be some benefit in disentangling the provisions so as to make their effect clearer.
- 2.15.25 The provision, in so far as it relates to principle 11, has been derived from a much clearer provision in the Privacy of Information Bill. The disclosure principle in the bill originally provided, before the material was amalgamated into section 7, that:
- “(2) Nothing in subclause (1) of this principle shall be taken as authorising the disclosure of any personal information in any case where the disclosure of that personal information would be a breach of any obligation of secrecy or non-disclosure imposed by the provisions of any enactment.”¹⁰⁷
- 2.15.26 The importance or potential of such a provision becomes clearer in that form. Expressed in the original manner the provision does not simply save the effect of other laws but also clearly precludes an agency from relying upon an exception to the disclosure principle in a case where a secrecy or non-disclosure provision constrains disclosure beyond what would otherwise be permitted. This

¹⁰⁶ Privacy of Information Bill, clause 32.

¹⁰⁷ Privacy of Information Bill, section 8, principle 14(2).

would appear to mean that an interference with privacy involving a disclosure of personal information may encompass a disclosure outside the bounds of principle 11 as restricted by the provision of another statute. This, to my mind, is a desirable state of affairs if Parliament's will in enacting secrecy or non-disclosure provisions, are to be given effect to and individual privacy respected.

- 2.15.27 For example, say a statutory health agency is obliged by a provision in an enactment to protect sensitive medical information on a database that it operates and not to disclose the information except to, say, a single statutory official. It transpires, on a complaint, that the information was disclosed in identifiable form in breach of the enactment to drug companies, politicians or researchers. In such circumstances, the original formulation that appeared in the Privacy of Information Bill would preclude the agency from seeking to argue that the disclosure was a “directly related purpose” or for “research purposes” etc.
- 2.15.28 The issue has been examined in Australia by a committee of the House of Representatives which had inquired into the protection of confidential information held by the Commonwealth Government.¹⁰⁸ That report noted that information privacy principles 10 and 11, which are similar to our own, set a weak minimum standard that is largely inadequate for confidential information. The Standing Committee stated:

“The Committee agrees where specific legislation contains express secrecy provisions the Privacy Act should not be used to expand the access that is otherwise permissible. To do so would undermine the protections expressly provided by the secrecy provisions and would allow a distortion of the protected purpose of the Privacy Act.”¹⁰⁹

The Committee recommended that the Australian Privacy Act be amended to provide where an Act other than the Privacy Act deals expressly with a matter of permissible use and disclosure, information privacy principles 10 and 11 do not operate to provide additional grounds for disclosure.

- 2.15.29 In my view, this is essentially what the original provision in the disclosure principle in the Privacy of Information Bill would have achieved. It appears that without necessarily intending to depart from that objective, the matter has become confused through its transfer into section 7 and amalgamation with a savings provision concerning principle 6. In my view, the matter is best resolved in relation to principle 11 by:
- disentangling the principle 11 issues from the principle 6 issues in section 7(2) and (3);
 - dealing with the effect of secrecy or non-disclosure provisions in all enactments identically and not distinguishing between statutes and regulations;
 - drafting the provision in a straightforward manner whereby its effect is plain; and
 - transferring the brief resulting provision into principle 11 itself so that its existence will more readily be brought to the attention of users of the principle.
- 2.15.30 It appears to me that the objective can be readily achieved by simply reverting to the formulation used in the Privacy of Information Bill.

¹⁰⁸ House of Representatives Standing Committee on Legal and Constitutional Affairs of the Parliament of the Commonwealth of Australia, *In Confidence: A Report of the Inquiry Into the Protection of Confidential Personal and Commercial Information Held by the Commonwealth*, June 1995

**RECOMMENDATION 33**

Section 7(2) and (3), in so far as they relate to information privacy principle 11, should be repealed and replaced with a single provision, which may be relocated into principle 11 itself, to the effect that where another enactment imposes a more restrictive obligation of secrecy or non-disclosure than principle 11, the principle does not operate to provide additional grounds for disclosure.

- 2.15.31 Section 7(2) and (3), once the material concerning principle 11 has been omitted, may simply be transferred into Part IV or may remain within section 7. However, I suggest that consideration ought to be given to restricting the effect of section 7(3) so as to increase the access rights of individuals.
- 2.15.32 When the Official Information Act 1982 was introduced it was a significant freedom of information inroad, preceded only by the Wanganui Computer Centre Act 1976, into a general regime of secrecy under the Official Secrets Act 1951. It was therefore quite understandable that a cautious decision was taken to save the effect of restrictive provisions in other enactments which were more narrowly focused than the all embracing Official Secrets Act. However, it was recognised that a culture of “open government” could be set back if a series of new restrictions could be introduced by regulation. Accordingly, while the effect of all other statutes was saved, only those regulations in force when the Official Information Act commenced were saved. The Danks Committee stated:

“As we have already mentioned there are, aside from the Official Secrets Act, many other statutes which provide protection for specific areas of information as well as sanctions for unauthorised disclosure. It is not uncommon for protection clauses to be included in new enactments. One result the Committee would not wish to see arising from the changes recommended in this report, would be a rash of new protective measures. This would, we consider, seriously undermine the Government’s intention and we hope it can be resisted. *The compatibility of protection accorded by existing statutes with proposals we are developing should be reviewed in due course.* This review will be part of the work programme of the new machinery we are proposing.”¹¹⁰

- 2.15.33 A review of statutes was part of the work programme of the Information Authority although there has been some criticism of the limited scope of the actual work undertaken (extending, for example, solely to enactments affecting “official information” as that term was then used in the Official Information Act and therefore not extending to the full range of information held by public bodies subject to the official information statutes following the 1987 extensions).

Restrictions on access in regulations

- 2.15.34 For the last 15 years the Executive has been constrained from creating new withholding provisions by regulation. The basic prohibition as it applies to information held by government departments was since extended in 1987 to other parts of the public sector and to local government. Since 1993 there has been a constraint upon using regulations to provide further reasons to withhold information which is held in the private sector. In my view, it is timely to consider removing regulations as a reason for refusing personal access requests.
- 2.15.35 My proposal is that a sunset clause provide that section 7(3) will expire after three years. The three year period would allow affected agencies, if they wished, to:
- identify any provisions in regulations upon which they rely to withhold infor-

¹⁰⁹ *Ibid*, page 64.

¹¹⁰ Committee on Official Information, *Towards Open Government: General Report*, 1980, page 28.



- consider whether the provision continues to be necessary and, if so, for equivalent provision to be made in primary legislation.

There would be no need to review the entire series of regulations in my view. Departments which know that they rely upon the regulations may review their options. Others will, I am sure, be quite able to operate without section 7(3), just as they do with post-1993 regulations.

- 2.15.36 Consultation did not bring forward any instance of regulations which are relied upon by agencies pursuant to section 7(3) in circumstances where withholding under Part IV would not be possible.¹¹¹ Nor have any complaints been brought to me concerning circumstances in which reliance has been placed upon section 7(3).
- 2.15.37 The regulations in issue, particularly those relating to section 7(3)(a)(i), were made at a time in which there were no relevant enforceable rights of access to personal information. In other words, they were crafted prior to the emphasis upon “open government” and accountability, in information terms, to the individual about whom information is held. It is desirable, in my view, that the public policy underpinning them as authority for refusing access should be reconsidered in today’s environment.
- 2.15.38 I see my proposal as being in keeping with the continuing review envisaged by the Danks Committee and the notion espoused in the Official Information Act of “increasing progressively the availability of official information to the people of New Zealand.”



RECOMMENDATION 34

A sunset clause should provide for the expiry of section 7(3) after a period of 3 years.

Restrictions on access in other statutes

- 2.15.39 Secrecy provisions are a traditional matter of concern for anyone interested in laws governing access to information. For example, the Information Authority made a study of them in the 1980s and, more recently, a similar review of secrecy provisions was carried out in respect of all statutes in Queensland.¹¹² I could not complete discussion of section 7 without noting that there continue to be certain statutory secrecy or non-disclosure provisions, the effect of which is saved by section 7(2), which appear to be unnecessarily restrictive when it comes to an individual exercising their rights of access under principle 6.
- 2.15.40 Secrecy or non-disclosure provisions in statutes and regulation have a role notwithstanding that the Official Information Act and Privacy Act deal with many information access and disclosure matters. For example:
- a statutory non-disclosure provision may be necessary so as to deny access to a class of documents or information in the event of an access request under the Official Information Act - although it is, of course, essential that such provisions be enacted sparingly and only in appropriately justified circumstances. Otherwise the integrity of the access entitlements under that statute will be eroded;
 - to constrain, consistent with public policy, the disclosure of particular types of information by agencies or employees of agencies;
 - to enable an agency to withstand a demand from another public agency - for example, enabling individual tax records to be held off limits to statutory requisitions from other departments or from Ministerial requests.

¹¹¹ Although some submissions asserted that relevant regulations may exist. See submissions M11 and S20.

¹¹² Queensland Law Reform Commission, *Freedom of Information Act 1992: Review of Secrecy Provision Exemption*, March 1994.

- 2.15.41 While I certainly accept the case for secrecy or non-disclosure provisions in appropriate circumstances, the provisions are often expressed in such a broad fashion that they sometimes unintentionally oust rights of access by the individual concerned. Often the need which led to the enactment of a secrecy provision had nothing to do with denying access to personal information by the individual concerned but that can be the effect. In my view, the tax legislation is an example of this. There is a very strong case for there to be a secrecy provision in the Tax Administration Act. However, I am not convinced of the need for that to be written in such a way as to deny an individual's right of access to information held about him or her.¹¹³ Another example is the secrecy provision which applies to the Police Complaints Authority. I have been concerned at a recent case which has the effect of allowing that secrecy provision to effectively deny individual access to a class of information.¹¹⁴ I accept that there will be many cases in which both the IRD and the Police Complaints Authority will, entirely appropriately, withhold information from a requester. However, the withholding grounds in the Privacy Act are, in my view, quite sufficient to achieve that purpose. My concern is that the secrecy provisions unnecessarily oust the access regime including independent review of a decision to withhold.¹¹⁵
- 2.15.42 Departments which administer statutes containing secrecy provisions should consider whether they ought to be reviewed so that the effect on individual access requests (as against Official Information Act requests) are not unnecessarily precluded. For the most part, this could be achieved by including an exception in the secrecy provision allowing disclosure to the individual concerned. In other cases, where it is intended that certain classes of information be withheld from the individual concerned, this may be provided in a way that the individual access entitlements continue for the balance of information held.

The rump of section 7

- 2.15.43 Section 7 has a central place in the present scheme of the Act. With the changes that I have recommended it will become a much smaller and less important provision. However, there also remains the possibility that some of my recommendations will be acted upon and not others. I have deliberately presented the suggestions in a manner whereby it is possible to avoid an "all or nothing" choice. It may therefore be useful to briefly mention what might be left of section 7 when most or all of my recommendations are taken into account.
- 2.15.44 Section 7 will roughly appear as follows:
- section 7(1):
 - as it relates to principle 6, retained as it is;
 - as it relates to principle 11, omitted, with the content transferred as an exception into principle 11;
 - section 7(2) - omitted, with the content distributed as follows:
 - as it relates to principle 6 - transferred into Part IV as a reason for refusing a request for access;
 - as it relates to principle 11, combined with relevant material from section 7(3), and transferred in redrafted fashion to principle 11;
 - section 7(3) omitted, and transferred as follows:
 - as it relates to principle 6, into Part IV together with section 7(2);
 - as it relates to principle 11, combined with section 7(2) as a

¹¹³ I have taken up these concerns in my Report to the Minister of Justice on Clause 81 of the Tax Administration Bill, October 1994.

¹¹⁴ See *Attorney-General v The District Court at Nelson*, 29 June 1998 (CA215/97).

¹¹⁵ Albeit that the exercise, or non-exercise, of the discretion to disclose may be a matter amenable to review by the courts or Ombudsmen.

new part of principle 11 or as a part of section 7 disentangled from access issues;

- section 7(4) omitted, by variously dispersing the provision as exceptions to the relevant principles or, on a more modest reform, by dispersing some of the content as exceptions and retaining the balance in section 7;
- section 7(5) retained in section 7 or alternatively relocated with the specific exemptions found in Part VI;
- section 7(6) - omitted, by transferring a redrafted provision into section 8.

2.15.45 Depending upon what material is retained a suitably descriptive new marginal note may be adopted.

2.16 SECTION 8 - Application of information privacy principles

2.16.1 This section provides for the application of the information privacy principles. Subsections (1) to (3) set out the application of principles 1 to 11 to information collected or obtained before or after the commencement of the Act while subsections (5) and (6) set out the application of principle 12 to unique identifiers assigned before or after the Act's commencement.

2.16.2 Subsection (4) provides that nothing in principle 3 applied to the collection by means of a printed form so long as the form was printed before the commencement of the Act and was used before 1 July 1995. This was one of the measures to phase in the requirements of the Act in order to minimise compliance costs and disruption to businesses.

2.16.3 The provision has been considered in a Complaints Review Tribunal case but has not caused any difficulty in operation.¹¹⁶

2.17 SECTION 9 - Postponement of application of principle 11 to lists used for direct marketing

2.17.1 Section 9, like section 8(4), assisted in the phase-in of the application of the Act. It allowed the continued disclosure by direct marketers of personal information, particularly names and addresses, on existing lists until 1 July 1996, without having to obtain the authorisation of the individuals concerned. This provided a “breathing space” whereby direct marketers could, for example, contact individuals on such lists and inform them of their options, such as to remain on the list or to be removed, to begin the construction of brand new lists in conformity with the collection principles.

2.17.2 I believe that the provision was successful in easing the position of direct marketers enabling them to make the transition from “anything goes” to one in which complaints could be brought under the new law. The transitional provision was appreciated by the practitioners of direct marketing and list brokers. It provided an opportunity for the NZ Direct Marketing Association to inform its membership as to the requirements of the new Act and to assist in compliance programmes.

2.17.3 One unfortunate misunderstanding, which was not entirely dispelled by the active efforts of the NZDMA in training, was that direct marketers were somehow exempted from the Privacy Act until 1 July 1996. It is plain that the section only has relevance to principle 11 and, for example, the collection principles applied from the commencement of the Act as with other agencies. It remains a disappointment to me that there continues to be considerable non-compliance, or only partial compliance, with agencies collecting personal information for direct marketing purposes. Competing priorities have prevented

¹¹⁶ *Powell v Special Education Service*, Complaints Review Tribunal, 26 July 1996, CRT Decision No. 26/96.

me from undertaking compliance monitoring work in this area but the NZDMA has made positive efforts to encourage compliance.

2.18 SECTION 10 - Application of principles to information held overseas

- 2.18.1 Section 10 provides that information held by an agency includes information held by that agency outside New Zealand. For the purposes of principles 5, 8, 9, 10 and 11, the information in question must have been transferred out of New Zealand. For the purposes of principle 6 and 7, all personal information, whether or not it was transferred out of New Zealand, is covered. An immunity is extended to breaches of the information privacy principles outside New Zealand that result from an agency's compliance with foreign laws.
- 2.18.2 The provisions seek to prevent non-compliance with the information privacy principles by agencies that might be tempted to move their holdings of personal information overseas. This is relevant to the problem of so-called "data havens". It is possible that section 10 also offers some reassurance to countries transferring personal information to New Zealand that any further transfer on to a third country will not deprive the information of the Privacy Act's safeguards. However, the section does not adequately deal with the problems of the transfer of New Zealanders' information to data havens nor the routing of personal data through New Zealand on to another agency in a data haven. I mention these issues below in the context of a proposal directed to controls on transborder flows of personal information.
- 2.18.3 However, section 10 also has a far more mundane objective which has nothing to do with concerns about agencies which would deliberately transfer information into a jurisdiction without privacy laws so as to avoid the controls of the Act or any other data protection law. Rather, it is a fact of life that some businesses operate across national boundaries and, without any wish to circumvent the law, may move information overseas to use or process it. A current example concerns the position of banks operating in New Zealand. Nearly all banks are now foreign owned and several of these have their head office in Australia, a jurisdiction having no general privacy laws covering the private sector.¹¹⁷ It has been reported, for example, that the Bank of New Zealand is relocating its data processing centres to Melbourne.¹¹⁸ While the information remains held by the BNZ section 10 requires that the information must be held securely as required by principle 5 and held, used and disclosed only in accordance with principles 8 to 11. It also means that BNZ customers can continue to exercise their rights of access and correction under principles 6 and 7. It does not cover information disclosed to, and thereafter held by, another agency in Australia in a way which would give remedies to a New Zealand customer who may be affected.

Transborder data flows

- 2.18.4 I have come to the conclusion that section 10 alone is not adequate for dealing with issues of "data export" or "transborder data flows". In making a proposal for change I have carefully considered the international dimension, particularly the OECD guidelines and also New Zealand's position as a "third country" in respect of the EU Directive on data protection. I have also been mindful of the fact that transborder data flows have been an issue in a variety of ways during the last five years and this may increasingly be the case. For example, transborder data flows issues have arisen in a variety of my functions such as:
- responding to enquiries - for example, recent public concerns at the sale of

¹¹⁷ Part IIIA of the Privacy Act 1988 (Australia) will apply to Australian banks as "credit providers". However, that Part is not equivalent to a general privacy law but has relevance only to some aspects of credit reporting by credit reporting agencies.

¹¹⁸ "BNZ Data Processing Goes Offshore," Infotech Weekly, The Dominion, 31 May 1998.

large quantities of valuation data to a company in Queensland;¹¹⁹

- my complaints function - for example, involving the transfer of a man's HIV details to a Pacific Island country resulting in adverse action against the individual;¹²⁰
- examining legislative proposals - for example, I have formally reported to the Minister of Justice in respect of transfer of information pursuant to the Passports Act and Trans-Tasman Mutual Recognition Act and have examined legislation for the transfer of customs information to overseas agencies;¹²¹
- my code of practice function - I have imposed some relevant controls in the context of the privatisation of the Government Computing Service which was responsible for data processing in respect of the law enforcement and taxation systems.¹²²

I also received a number of submissions during consultation on this review on the subject of transborder data flows.¹²³

- 2.18.5 In the material that follows I outline the international approach, and the approach taken in several jurisdictions, to the question of transborder data flows. I then make a proposal for how the matter might appropriately be addressed in New Zealand.

International approaches to transborder data flow issues

- 2.18.6 Transborder data flows were the prime reason for the involvement of the OECD in privacy issues. The approach of the OECD is illustrated by the preamble to its 1980 Guidelines which recognised that:
- although national laws and policies may differ, member countries have a common interest in protecting privacy and individual liberties, and in reconciling fundamental but competing values such as privacy and the free flow of information;
 - automatic processing and transborder flows of personal data create new forms of relationships amongst countries and require the development of compatible rules and practices;
 - transborder flows of personal data contribute to economic and social developments;
 - domestic legislation concerning privacy protection and transborder flows of personal data may hinder such transborder flows.

- 2.18.7 The 1981 Council of Europe Convention No 108 also recognised in its preamble the necessity to reconcile “the fundamental values of the respect for privacy and free flow of information between people.” In 1991 the Council amplified its approach by issuing recommendations recognising that personal data should not be transferred into states which “are not in conformity” with the Convention unless necessary measures have been taken to respect principles in the Convention such as:

- contractual provisions reflecting Convention principles and with the data subject given the possibility to object, or;
- obtaining the data subject's free and informed consent in writing.¹²⁴

The recommendations also suggest that measures should be taken to avoid data

“A member country should refrain from restricting transborder flows of personal data between itself and another member country except where the latter does not yet substantially observe these guidelines or where re-export of such data would circumvent its domestic privacy legislation.”

- OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA, 1980

¹¹⁹ See, for example, “Ombudsman Order Freed Home Details”, *New Zealand Herald*, 26 June 1998.

¹²⁰ See case note no 6998. Another complaint, still under investigation, concerns a joint Australia-New Zealand agency which stores its New Zealand records in Australia and which has claimed therefore that the information is unavailable to the individual seeking access.

¹²¹ See Report of the Privacy Commissioner to the Minister of Justice on the Passports Bill, July 1992, and on the Trans-Tasman Mutual Recognition Bill, April 1997.

¹²² See GCS Information Privacy Code 1994 and EDS Information Privacy Code 1997.

¹²³ See submissions R1-R8, R12-R14, G6, G10, G13, G14, G17-G19, G21, S2, S11, S37, S42 and S45.

¹²⁴ Council of Europe, Recommendations on Communication to Third Parties of Personal Data held by Public Bodies, Recommendation R(91)10, September 1991.

being subject to automatic transborder communication without the knowledge of the individuals concerned.

- 2.18.8 A similar approach to that taken by the OECD and Council of Europe was taken in 1990 United Nations Guidelines for the Regulation of Computerised Personal Data Files. Accordingly, during the 1980s and early 1990s, the international approach to the issue of transborder data flows has been to encourage consistent privacy law in jurisdictions which may transmit, receive or process personal data, and so long as the relevant privacy laws are comparable, to thereby avoid the need to place any additional restrictions on transborder data flows.
- 2.18.9 However, the international instruments all recognise that controls may be appropriate in two exceptional cases:
- where a recipient country does not “substantially observe” the guidelines (the OECD terminology), where there are no “reciprocal safeguards” (UN) or where there is no “equivalent protection” (Council of Europe);
 - where the exported data is routed through an intermediary country with satisfactory privacy laws in an attempt to circumvent the originating country’s privacy laws: “where the re-export of such data would circumvent its domestic privacy legislation” (OECD) or “where the transfer is made ... through the intermediary of the territory of another party in order to avoid such transfers resulting in circumvention of the legislation” (Council of Europe).
- 2.18.10 Clause 17 of the OECD Guidelines provides in full:

“A member country should refrain from restricting transborder flows of personal data between itself and another member country except where the latter does not yet substantially observe these guidelines or where the re-export of such data would circumvent its domestic privacy legislation. A member country may also impose restrictions in respect of certain categories of personal data for which its domestic privacy legislation includes specific regulations in view of the nature of those data and for which the other member country provides no equivalent protection.”

- 2.18.11 The emphasis given in the respective OECD and European instruments has meant that most European privacy laws contain express transborder data controls whereas most laws based on the OECD Guidelines (like New Zealand) do not. Section 12 of the Data Protection Act 1984 (UK) for example, implemented the Council of Europe Convention, by giving the UK Data Protection Registrar (equivalent to the Privacy Commissioner) a limited power to prevent personal data being transferred to a place outside the UK if satisfied that there is likely to be a contravention of one of the data protection principles as a consequence of the transfer.

EU Directive and transborder data flows

- 2.18.12 Interest in the matter of transborder data flows was rekindled in the 1990s through the involvement of the European Union in privacy matters. The EU’s approach has changed the relatively relaxed way that the OECD and other bodies tackled the issue. Article 25 of the EU’s 1995 Directive provides that EU countries *must* provide that the transfer of personal data to third countries for processing may take place only if the third country ensures “an adequate level of protection”. The importance of the EU in international trade has meant that this requirement has refocused attention in a number of countries on whether their laws would be adequate in European eyes and also whether their own approach to data exports is appropriate.

2.18.13 Transborder controls are being re-evaluated in EU countries which need to implement the directive in national law. Section 12 of the Data Protection Act 1984 (UK) is inadequate to meet the Directive’s requirements. Instead a new data protection principle has been proposed which states:

“Personal data shall not be transferred to a country or territory outside the European Economic Area unless the country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.”¹²⁵

2.18.14 Jurisdictions outside Europe are looking to the possibility of transborder data flow controls not simply to protect the data of their own citizens but also to ensure that their jurisdictions are not perceived as conduits for transfers to “data havens” for which direct transfers would be banned. Hong Kong, Quebec and Taiwan have already adopted controls.

2.18.15 The transborder data flow controls in section 33 of the Hong Kong law only take effect if the Hong Kong Ordinance ceases to apply.¹²⁶ Where the transfer of data is accompanied by a loss of control of the data, section 33 applies. This permits a transfer where it is to a jurisdiction possessing “any law which is substantially similar to, or serves the same purpose as, this Ordinance” and the Privacy Commissioner may specify such jurisdictions by Gazette notice. Also permitted are transfers justifiable on public interest grounds, or which further the interest of the individual concerned. In all other cases section 33 subjects the transferor to a duty to take all reasonable steps to ensure that the transferee applies similar data privacy standards to those applicable in Hong Kong. It is for the transferor to assess the situation and take the most appropriate steps. Consideration has to be given to such measures as obtaining contractual assurances and in this respect the Hong Kong Commissioner has released model contractual conditions.¹²⁷ The Commissioner can receive complaints relating to an alleged breach of the transferor’s duty. The Hong Kong prohibitions are enforced by an enforcement notice procedure.

2.18.16 In my view, the Privacy Act should be amended to address more precisely the circumstances in which transborder data flows should be prohibited or subjected to additional controls. In doing so it is unnecessary to adopt the restrictive EU model which has also been adopted in Hong Kong. New Zealand is a not member of the European Union and it is the OECD Guidelines to which we should primarily direct our attention. However, the EU Directive *is* relevant in so far as it is desirable to make sure that the New Zealand law, in the context of any transborder data controls, offers “adequate protection” in EU eyes. By this, I mean that any controls adopted should be able to be utilised in circumstances where it appears that a European data controller is transferring information using New Zealand as an intermediary in an attempt to circumvent European laws.

2.18.17 In this regard, I draw attention to the fact that Europeans might consider New Zealand’s law contains no effective restriction on onward transfer in such circumstances. Restrictions on onward transfers have been suggested as a “core

¹²⁵ Data Protection Bill [HL] (UK), introduction version, Schedule 1 (Part I), principle 8. The scheme is further spelt out in the second part of Schedule 1 and in Schedule 4.

¹²⁶ To relate this to a New Zealand situation, section 10 of the Privacy Act 1993 makes it clear that the privacy principles continue to apply to certain information held by New Zealand agencies overseas. If the Hong Kong approach were to be taken, any special transborder data flow controls would only apply if the New Zealand agency relinquished control in terms of section 10.

¹²⁷ Office of the Privacy Commissioner for Personal Data, Hong Kong, fact sheet no 1, “Transfer of Personal Data Outside Hong Kong: Some Common Questions”, May 1997.

principle” for assessing the existence of “adequate protection” in a particular jurisdiction.¹²⁸ One commentator has already suggested that the core principle concerning restrictions on onward transfers is a logical closing of a loophole which could otherwise be used to circumvent the restrictions on transfers from the EU by an intermediate transfer through a “safe” third country. The same commentator has suggested that the principle weakens the case for adequacy of what is otherwise one of the strongest privacy laws outside Europe, that of New Zealand.¹²⁹

Transborder data flow proposal

- 2.18.18 It should be possible to create a mechanism to control or prohibit the export of personal information in circumstances where an official body from a country having export controls compatible with the OECD approach requests New Zealand to take action in respect of a particular transfer of information utilising New Zealand as a conduit to circumvent its own privacy laws. The resultant provision might resemble “mutual assistance” provisions found in other contexts. The enforcement mechanism might be modelled upon the “transfer prohibition notices” provided for in section 12 of the Data Protection Act 1984 (UK). If this approach were to be taken there would be a number of issues to be worked through such as:
- which official requests are to be recognised - the mechanism would need to work for both European and non-European countries and be compatible with the OECD approach;
 - whether the transfer prohibition notice is to be a function exercised by the Privacy Commissioner (as it is in the UK), the government (by Order in Council, Ministerial Order, Gazette Notice etc) or on application to the courts or Tribunal;
 - the precise effect of such a notice and what steps the agency is required to take so as to resume the data exports;
 - whether there are to be appeal mechanisms and, if so, whether the Complaints Review Tribunal should be used.
- 2.18.19 If there are to be express controls on transborder data flows it would seem anomalous to give special protection to the information flowing through New Zealand from other countries and not consider the position of information about New Zealanders themselves. Again, I do not suggest that the restrictive approach of the EU Directive be adopted as I believe that principle 11 taken together with section 10 provides, for the most part, an adequate framework. However, I believe that these would be enhanced by the addition of controls which could be exercised in exceptional cases through:
- a transfer prohibition notice - of the type existing in section 12 of the Data Protection Act (UK) and suggested above as a means to counter the use of New Zealand to circumvent other countries’ data export controls; and
 - a code of practice.
- 2.18.20 I have not attempted to draft a transborder data flow provision, but have instead indicated my support of such a provision or provisions and indicated the elements I believe should be incorporated. The proposal that I have made is for a transborder data flow control at the “weaker” end of the scale. It is intended to be one step along from having no such controls at all. We live in an increasingly globalised environment and I have no wish to create excessive or unnecessary barriers to transborder data flows. As already observed the OECD Guidelines attempted to avoid such barriers although acknowledging the legitimacy

¹²⁸ See Working Party on the Protection of Individuals with regard to the Processing of Personal Data, Reflections on Transfers of Personal Data to Third Countries - Possible ways forward in assessing adequacy, June 1997, clause 3(i)(6).

¹²⁹ Graham Greenleaf, “The European Union’s Privacy Directive - New Orientations on its implications for Australia”, Australian Privacy Summit, Sydney, October 1997.

of controls in some circumstances. However, I believe that it will be increasingly untenable to maintain a privacy law with no mechanism at all for data export controls. The emphasis I have placed in my proposal is on the creation of a mechanism for use in *exceptional* circumstances. In this respect, the proposal differs significantly from that adopted in the European Union and Hong Kong. The exceptional cases include attempts to circumvent EU controls and therefore the proposal will work in harmony with the EU Directive and rebut any suggestion that New Zealand’s law should be seen as “inadequate”.



RECOMMENDATION 35

The Act should be amended to include express provision for controlling transborder data flows, consistent with clause 17 of the OECD Guidelines and the emerging international approach to data export. In particular, consideration should be given to providing:

- (a) a mechanism which would enable mutual assistance to be extended to prohibit data exports in circumstances where New Zealand is being used as a conduit for transfers designed to circumvent controls in EU and other privacy laws;
- (b) mechanisms for imposing restrictions concerning categories of personal information for which there are particular sensitivities and in respect of which the recipient countries would provide no adequate protection.

2.19 SECTION 11 - Enforceability of principles

2.19.1 Section 11 provides that where a public sector agency holds personal information, the individual concerned has a legal right of access under principle 6 that may be enforced by court order. However, in relation to information held by private sector agencies one must work through Part VIII of the Act for enforcement of an individual’s principle 6 entitlement.

2.19.2 The intent of section 11 was to preserve existing legal rights conferred by the Official Information Act. The position was taken that a right conferred by statute should not lightly be taken away. However, it was not considered appropriate that the access entitlement in relation to private sector agencies be directly enforceable through the courts. It was recognised that a more cost effective way of enforcement is through investigation and conciliation by an independent public official who specialises in information privacy. There was generally little support in submissions for giving the ordinary courts a greater jurisdiction to consider complaints of interference with privacy.¹³⁰

2.19.3 The position is generally satisfactory in principle from my perspective. One problem in operation has been that due to the base funding of my office being outstripped by the volume of complaints I have had to queue complaints. That of itself does not provide a good reason to change the balance struck in section 11 which remains, in my view, sound. However, it does reinforce another one of the unfortunate consequences of a lengthy complaints queue which is to place some complainants in a favourable position by allowing the possibility of “jumping the queue” to seek an enforceable order through the courts.

Private prosecutions

2.19.4 Notwithstanding the existence of the right to enforce access rights to information held in the public sector through the courts, the right is rarely exercised except in one circumstance. The one circumstance involves the individuals

¹³⁰ Eleven submissions opposed extending the jurisdiction of the courts (see submissions UV3-UV5, UV8, UV10-UV13, UV16, S36 and S46). Three submissions thought that the courts should have a further role (UV1, UV6 and S42). One explained that complainants should be able to select a wider range of complaint avenues (UV1) and another thought the courts should be able to hear access or disclosure complaints after the Commissioner’s processes were complete (UV6).

“The courts, like the Ritz Hotel, may be open to all but only a few can afford the rooms. It not surprising that no individual requester of personal information has taken the matter to court.”

- EAGLES, TAGGART LIDDELL,
FREEDOM OF INFORMATION IN NEW
ZEALAND, 1992

who have been charged with an offence. Essentially principle 6 rights are the basis for the accused person to have access to personal information held on prosecution files.¹³¹ This right is enforced through the courts.

- 2.19.5 The current arrangements for having access to information in the course of criminal proceedings is not perfect. For that reason a proposal is being studied to create a specific statutory criminal disclosure regime.¹³² In the medium term there is therefore the prospect of important enhancements to the processes. However, in the meantime the Privacy Act access regime underpins the criminal discovery process. In the light of that, I have some concerns as to the limitation of legal rights in cases where a prosecution is brought by an agency which is not a “public sector agency”. Although such prosecutions concern a tiny proportion of all prosecutions brought, they are by no means unknown. For example, I understand that both the NZ Law Society and the SPCA occasionally bring prosecutions but neither are “public sector” bodies for purposes of the Privacy Act. Nor are they subject to the access regime in the Official Information Act. There has also been talk recently of the prospect of more private prosecutions being brought than has hitherto been the case.
- 2.19.6 Where private sector agencies bring prosecutions they will be subject to information privacy principle 6. The accused person is entitled to seek access to information held by such agencies so as to help prepare a defence. However, the issue is not the direct applicability of information privacy principle 6 to the agencies bringing private prosecutions but whether *the courts* can enforce those entitlements. It appears from section 11 that they cannot.
- 2.19.7 The individual could enforce the access entitlements through parallel processes involving my office and the Complaints Review Tribunal but this would not be satisfactory, particularly if court proceedings progress at a different pace from complaints processes carried out under the Privacy Act (which is quite likely with the current complaints queue).
- 2.19.8 I suggest therefore that section 11 should be amended so as to extend the entitlements which are “legal rights” beyond those presently specified in section 11(1) to include the entitlements conferred by principle 6(1) in so far as they relate to personal information held by an agency, which is not a public sector agency, where that agency has initiated criminal proceedings against the individual. I believe that the change is warranted so as to ensure that the accused person’s rights are not diminished merely by the status of the person bringing the prosecution and to ensure that the courts have the necessary powers to supervise the process.



RECOMMENDATION 36

Section 11 should be amended so that the entitlement under information privacy principle 6(1) to have access to information held by an agency is a legal right in circumstances where the agency is prosecuting the individual for an offence.

¹³¹ The resultant process, sometimes referred to as “criminal discovery” (to equate with the “discovery” process used in civil proceedings), also involves the court exercising jurisdiction in relation to the Official Information Act and common law obligations.

¹³² See Ministry of Justice and Department for Courts, Consultation paper regarding Preliminary Hearings And Criminal Disclosure, October 1997.

Part III

III

Privacy Commissioner

109

“The matter is too important to leave in the hands of any government. The Government is placing an independent party in that role - a man or woman of integrity - to ensure that the provisions relating to privacy that Government members regard as important are strictly observed and policed.”

- Hamish Hancock MP, Second reading of the Privacy Commissioner Bill, November 1991

“Data protection commissioners are a form of highly specialised ombudsmen with a more active part to play than the classical role of responding to individual complaints. It is not enough to respond to repeated grievances from a changing cast of individuals. The staff has to pursue systematic improvements in information handling practices by using a variety of methods.”

- David Flaherty, *Protecting Privacy In Surveillance Societies*, 1989

3.1 INTRODUCTION

3.1.1 Part III of the Act provides for the appointment of a Privacy Commissioner and sets out the Commissioner’s general powers and functions.

3.1.2 An independent supervisory body is a common feature in many privacy and data protection laws. European data protection laws typically create a data protection commission or commissioner whereas the title of privacy commissioner has been preferred in Canada and Australia.¹ Many countries have found the creation of an independent Commissioner a vital part of a credible regime for the protection of privacy. The absence of a Privacy Commissioner in the USA has, in recent years, been repeatedly cited as a shortcoming in the adequacy of American privacy arrangements notwithstanding the existence of some strong privacy laws.²

3.1.3 The report which preceded the Privacy of Information Bill described what was to become the Privacy Commissioner as a “statutory guardian for privacy interests”.³ The Minister of Justice characterised the Commissioner as a privacy “watchdog”.⁴ The remark was made when noting that the Privacy Commissioner Bill would confer upon the Commissioner functions then exercised by the Human Rights Commission. In fact, a number of the Commissioner’s

¹ The title usually adopted at provincial level in Canada is “Information and Privacy Commissioner”.

² Including one of the world’s oldest privacy laws, the Privacy Act 1974 (USA).

³ Tim McBride, *Data Privacy: An Options Paper*, December 1987, paragraph 7.85.

⁴ Privacy Commissioner Bill, second reading, 26 November 1991.

functions were formerly exercised by the Human Rights Commission, Ombudsmen, Wanganui Computer Centre Privacy Commissioner and Information Authority. Most of the other functions mirror those exercised by other privacy and data protection commissioners.⁵ A few are unique to the New Zealand Act.

- 3.1.4 Part III comprises sections 12 to 26. I have reviewed all fourteen sections to see whether any amendment is necessary or desirable. I have, for example, considered whether:
- the provisions have operated satisfactorily in the last five years;
 - new functions would enable better protection of privacy or contribute to the reduction of compliance costs;
 - any of my functions would desirably be narrowed or removed.

SECTION BY SECTION DISCUSSION

3.2 SECTION 12 - Privacy Commissioner

- 3.2.1 Section 12 provides for the appointment of a Privacy Commissioner by the Governor-General on the recommendation of the Minister of Justice. This is the normal approach taken in New Zealand legislation for the appointment of Commissioners. In some comparable jurisdictions the Commissioner is an Officer of Parliament and therefore the appointment is by, or with the concurrence of, the relevant legislature.⁶

Officer of Parliament

- 3.2.2 Amongst comparable independent entities, the Ombudsmen, Commissioner for the Environment, and Auditor-General, are each Officers of Parliament. The Wanganui Computer Centre Privacy Commissioner was an Officer of Parliament from 1976 to 1993. On the other hand, the Human Rights Commissioners and Race Relations Conciliator, are not.

- 3.2.3 There is no statutory definition or criteria established to identify an Officer of Parliament.⁷ The status is one attached on an individual basis to particular positions as they are established. Nor is there any specific definition of what being an Officer of Parliament entails in respect of powers, duties and functions. However, typically one would expect the creation of an Officer of Parliament to be reflected in the appointment procedures, reporting arrangements and appropriation of funding.

- 3.2.4 The issue was considered by the select committee which studied the Privacy of Information Bill. That committee decided not to change the status of the Commissioner from that contained in the bill as introduced. Establishing the Commissioner as an Officer of Parliament is sometimes suggested as promoting the independence of the position. In my view, that concern is misplaced (except in the context mentioned in the next paragraph). I have not felt that my independence has been diminished by reporting primarily to the Minister of Justice rather than to a Parliamentary committee.⁸ Indeed, I have, for the most part, found the present arrangements satisfactory and appropriate.

- 3.2.5 However, I have one concern bearing upon independence and which is not

⁵ Particularly the Australian Privacy Commissioner since the Privacy Act 1993 is, in a number of respects, modelled upon the Privacy Act 1988 (Australia).

⁶ This is the approach taken in most Canadian jurisdictions.

⁷ Non-statutory attempts have been made to define when it is appropriate to confer on an official the status of "Officer of Parliament". See David McGee, *Parliamentary Practice in New Zealand*, 1994, page 55.

⁸ In any case, I feel that I have developed with the Minister a satisfactory *modus operandi* whereby any reports that are concurrently of interest to a select committee are usually copied by the Minister's office to the relevant committee.

“We believe that section 12 should be amended so that the Privacy Commissioner is appointed by Parliament rather than by the Minister so that they have more statutory independence and public and parliamentary accountability.”

- AUCKLAND DISTRICT
COUNCIL OF SOCIAL SERVICE,
SUBMISSION G6

faced by Officers of Parliament. The funding to carry out my various statutory functions is procured by the Ministry of Justice as a small component of Vote: Justice. The Ministry concurrently makes the case for its own spending and a variety of Crown entities it has responsibilities for. Expectations of the privacy legislation are, to a degree, being thwarted through inadequate baseline funding. I am somewhat frustrated by the situation where the merits of my case are argued in my absence by a Ministry whose funding for its own projects will, in general, be diminished by any additional funding devoted to my office. I suggest that an arrangement should be made for independent Commissioners in my position to be able to put aspects of their case for funding directly to the Treasury and Ministers.



RECOMMENDATION 37

There should be provision for the Commissioner to put a case for funding directly to Treasury and relevant Ministers.

Crown entity

3.2.6 Section 12(3) provides that the Commissioner is a corporation sole who has, for example, all the powers of a natural person. Section 12(4) establishes the Commissioner as a “Crown entity” for the purposes of the Public Finance Act 1989. “Crown entities” are a collection of public sector bodies which are at arms’ length from the Government, unlike departments, and brought together for the purposes of the Public Finance Act. They are not generally involved in trading activities. The functions of many Crown entities require a degree of independence from the Government.

3.2.7 One development in the last few years has been a debate over whether it is appropriate for Crown entities to enter into a contract with their respective Ministers. As this has been seen to impinge upon independence an alternative model has been developed involving the execution of Memoranda of Understanding (MOU) with Ministers. Before agreeing to my MOU I was very mindful of the possible effect upon the independence of the position and ensured that it was appropriately structured to avoid any problems.

3.3 SECTION 13 - Functions of Commissioner

3.3.1 Section 13 sets out the Privacy Commissioner’s principal functions. The list inevitably attracted criticism in some submissions on account of its length alone. However, I do not favour reformulation into a briefer, yet inevitably more vague, statement of functions. Although some of the functions appear to overlap with others, and a few have not been exercised, each fulfils an important purpose and should be retained. I am aware that in some jurisdictions the absence of a clear statutory function has meant that at critical times governments and agencies have been able to exclude projects from a Commissioner’s privacy scrutiny. On the other hand, for those people concerned at a Privacy Commissioner potentially going beyond an appropriate remit, the specificity of the functions gives good statutory guidance as to what a Commissioner may appropriately do.

Function (a): Education and publicity

3.3.2 My first function is to promote, by education and publicity, an understanding and acceptance of the information privacy principles and of the objects of those principles. The function interrelates with function (g) concerning education programmes.⁹

3.3.3 Education is essential for the protection of privacy in the 1990s and beyond. I am confident that all of my fellow Privacy Commissioners internationally would

⁹ See paragraph 3.3.43 - 3.3.46.

“The list of functions in section 13 is unusually long and does not give a sense of the core functions of the Commissioner.”

- NZ LAW SOCIETY PRIVACY WORKING GROUP, SUBMISSION G22

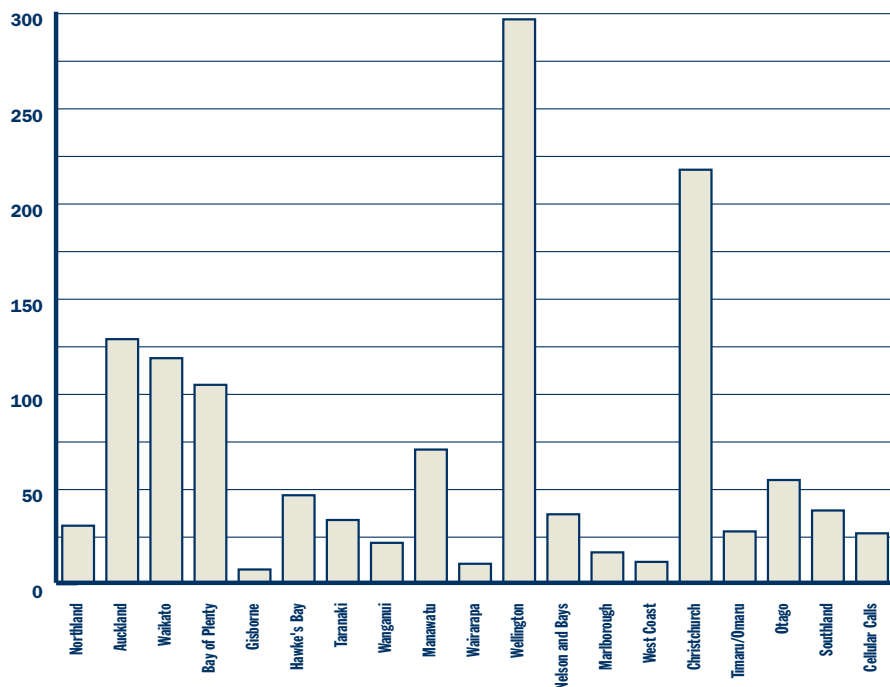
agree that the education of citizens and agencies about privacy risks and solutions is an absolutely essential part of the job. Given the new issues that continue to arise, and the rapid pace of technological development, it is vital that privacy issues be raised for public debate.

- 3.3.4 It may be valuable at this point to give something of an overview of the activities my office has undertaken in relation to carrying out the education and promotional functions. In the space available I can only point out some of the principal endeavours. Further details can be obtained from my annual reports.

Privacy hotline

- 3.3.5 Since 1993 I have operated a freephone privacy hotline staffed by 2, and later 3, officers who have in the main been legally qualified. This provides equitable access to the resources of my office throughout the country. The following graph shows the typical geographical spread of calls over a two month period.¹⁰

Figure 2: **Geographical spread of 0800 calls received in June/July 1997**



- 3.3.6 In a typical year my enquiries team handle over 8,000 telephone enquiries. The privacy hotline also acts as an entrance point to other resources of my office. For example, the enquiries team:
- distributes to enquirers many of the printed materials available from the office;
 - is often a contact point for consultations on codes of practice.

Written enquiries

- 3.3.7 All my professional staff are involved in responding to written enquiries from agencies and the public. However, the bulk of the general work is concentrated with my enquiries team which, during 1996/97, received 595 written enquiries.
- 3.3.8 As with the privacy hotline, written enquiries are an important entry point into other aspects of the office's work. For example, enquiries are made as to whether there are valid grounds for a complaint. In many cases, through the actions of the enquiries team problems are "headed off" so as to avoid a complaint. The office tries through responding to enquirers to give individuals and agencies the tools and information they need to sort out problems themselves.

¹⁰ Note that the graph displays calls into the 0800 number. It does not cover calls to the enquiries team on other numbers - such as those originating in Auckland.

"The Privacy Commissioner clearly needs more resources to train and inform agencies, so that they can comply more readily and more cheaply."

- AUCKLAND COUNCIL OF SOCIAL SERVICE, SUBMISSION WX8

Written publications

3.3.9 My office has an active publication and information dissemination policy. Key series of publications include:

- *fact sheets*: a series of short flyers outlining the key aspects of the legislation;
- *issues sheets*: canvassing topical matters and exploring issues under the privacy law;
- *compilations of materials*: speeches, reports, articles and the like, are brought together in a series of compilations which make them easily available. The eighth volume brought this up to December 1997. A series of specific compilations touch upon a variety of matters ranging from employment to information matching.¹¹

A variety of other series exist such as the Privacy Issues Forum conference papers and guidance notes on various matters. A number of one-off publications have been released, such as *Private Lives? A Discussion Paper on Disability and Privacy Issues*, and a set of Mental Health Guidance notes.

Newsletter

3.3.10 I have released *Private Word* approximately ten times a year since December 1995. Amongst other things it publicises the work of the office, advertises the availability of workshops and resources, reports on topical privacy issues, and provides a vehicle for responding to misinformation that may have appeared in the news media concerning the application of the Act.

Privacy Issues Forum

3.3.11 Since 1994 I have convened a series of Privacy Issues Forums. The emphasis is on discussion of privacy issues rather than a series of lectures from privacy experts. However, I have been delighted to host a series of eminent experts from New Zealand and abroad. Notable at the most recent Auckland forum was the participation of Justice Michael Kirby of the High Court of Australia. Justice Kirby, one of the world's foremost privacy experts, chaired groups which prepared OECD guidelines in 1980 and 1992. A valuable series of papers is one legacy of the Forums.

FIGURE 3. PRIVACY ISSUES FORUM

Year	1994	1995	1996	1997	1998
City	Auckland	Wellington	Christchurch	Auckland	Wellington
Attendance	134	170	185	158	170

Case notes

3.3.12 Currently my office receives over 1000 new complaints each year. The results of individual complaints are not generally made public. However, anonymised case notes are prepared for a selection of cases which raise interesting or important issues. I release these case notes individually, or in small batches, during each year so that they may be appropriately reported in the news media (generally and in trade journals in relevant sectors). The case notes are available free of charge on an individual or annual basis from my office and I place them on my website. I encourage their publication elsewhere and they are, for example, republished in Butterworths' *Privacy Law and Practice*. There is now a degree of guidance on a selection of cases upon which I have rendered opinions which helps understanding of the Act and the approach that I have taken.¹²



Three Australians: Cementing trans-Tasman privacy links are Justice Michael Kirby of the High Court of Australia, Nigel Waters of the Australian Privacy Commissioner's Office and Victor Perton MP of the Victorian Parliament, at the 1997 Privacy Issues Forum. PHOTO: OFFICE OF THE PRIVACY COMMISSIONER

¹¹ The range includes, for example, compilations on privacy impact assessment, archives and libraries, information matching and electronic road tolls.

¹² These case notes do not have a "precedent" value in legal terms but offer a guide as to how the Commissioner is likely to approach a similar case.

Internet

- 3.3.13 Launched at the 1995 Privacy Issues Forum, my Internet site is now an important part of my office’s dissemination of information.¹³ Most key documentation produced from my office can be obtained from the web site as an alternative to seeking printed copies. The site was used in the consultation process which led to this report. People could browse my site to read or download copies of the 12 discussion papers released in 1997. There was also a facility for lodging submissions by email.

Participation in conferences

- 3.3.14 I frequently speak at conferences, seminars and workshops, as do some of my staff. Where written addresses are produced for conferences these are brought together and republished in compilations so as to enhance the availability of that resource.

Co-operation with commercial publishers and journals

- 3.3.15 Private sector publishers have shown an interest in privacy issues. I have been able to contribute to several publications material which has been prepared for conferences or other purposes. An active association exists with three journals of particular relevance to privacy issues:

- *Privacy Law and Practice* - to which key documents are made available for republication;
- *Human Rights Law and Practice* - for which the office is identified as a specialist contributor; one of my staff acts a consulting editor;
- *Privacy Law & Policy Reporter* - the Assistant Privacy Commissioner is on the editorial panel.

Such publications contribute to better understanding amongst agencies and the public of the Privacy Act and privacy issues generally.

Code commentary

- 3.3.16 I have put considerable effort into preparing explanatory commentary for the codes of practice I have issued. Especially notable is the extensive commentary to the Health Information Privacy Code.

News media

- 3.3.17 There is no hard and fast line between education and publicity but the limitations of the news media mean that such activities fall more towards the publicity end of the scale. Although only brief messages can be usually given in the news media, their value is important as the publicity can reach vast audiences. Frequently, news media work arises in respect of particular issues and involves my being interviewed for TV or radio. Media activities also interact with function (h) which I discuss below.¹⁴ Some particular initiatives that I have taken in order to publicise the work of my office, and promote discussion and understanding of privacy issues:

- when visiting cities with talkback programmes I have made myself available to be interviewed on topical or local issues;
- during 1996 I wrote a weekly column in the *Sunday News* entitled “Privacy Matters” canvassing topical privacy issues in under 350 words;
- in 1997/98 I presented a monthly 20 minute RNZ National Radio discussion on privacy issues entitled “Speaking privately”;
- occasionally I have contributed 4 minute talks to “Sunday Supplement” on National Radio;
- I have made frequent contributions to *Employment Today* and written occasional features in newspapers.

Function (b): Audit of personal information

- 3.3.18 The international literature on data protection and the protection of individual

¹³ <http://www.privacy.org.nz>

¹⁴ See paragraphs 3.3.47 - 3.3.49.

“The discussion paper outlines initiatives taken by the Privacy Commissioner to inform and educate agencies and the public. Those measures are well intentioned but tend to mask the inadequacies of the legislation itself, especially its complexity, its drafting style, its organisation, and the lack of clarity in its relationship with other statutes.”

- NZ LAW SOCIETY
PRIVACY WORKING GROUP,
SUBMISSION WX12

privacy identifies the audit function as being of particular importance. Despite this, I have not yet found it possible to undertake audits pursuant to the function. I recount here some of the uses and benefits of auditing as an effective tool for privacy, the approach of some overseas laws and commissioners, and some of the constraints upon my undertaking audits.

Canada

- 3.3.19 In 1989 Professor David Flaherty, published *Protecting Privacy in Surveillance Societies*.¹⁵ This was the outcome of a number of years study of the data protection laws, and the work of the data protection agencies, in Germany, Sweden, France, Canada and the United States. One of the strong threads amongst Professor Flaherty's conclusions was the significant value of audits carried out by data protection agencies. The following gives a flavour of the conclusions:

“Data protection commissioners are a form of highly specialised Ombudsmen with a more active part to play than the classical role of responding to individual complaints. It is not enough to respond to repeated similar grievances from a changing cast of individuals. The staff has to pursue general systematic improvements in information-handling practices by using a variety of methods.

“The conduct of audits is one of the most important and least developed aspects of controlling surveillance. The Federal experience in West Germany and Canada demonstrates their centrality for the pursuit of statutory objectives. Both countries have created separate units for inspections to assist the staff members who specialise in particular types of systems.”¹⁶

- 3.3.20 Many Privacy Commissioners would share Professor Flaherty's views as to the value or potential of auditing. The under-resourcing of my office to handle the volume of complaints has meant that I have been unable to undertake certain discretionary functions conferred upon me, including auditing.
- 3.3.21 Professor Flaherty has left academia for a term as Information and Privacy Commissioner of British Columbia.¹⁷ Commissioner Flaherty has had the opportunity to put the ideas of Professor Flaherty into practice. Although the British Columbia Commissioner has strong powers of audit¹⁸ this does not mean that a heavy handed approach is taken. Commissioner Flaherty has, for the most part, chosen to do audits in a relatively informal manner involving on-site inspections. Commissioner Flaherty has described what is involved in a site visit:

Format for a site visit

“For the most part, site visits are conducted informally. Typically, the Commissioner and/or members of his staff make a pre-arranged visit to a public body to discuss freedom of information and privacy issues and to tour the facilities. The focus is on viewing and understanding the information flow processes and policies of the public body, particularly within its manual and computerised record areas.

¹⁵ David H Flaherty, *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada and the United States*, 1989.

¹⁶ *Ibid*, page 400.

¹⁷ In that capacity I invited him, as keynote speaker, to the Privacy Issues Forum held in Christchurch in 1996.

¹⁸ Freedom of Information and Protection of Privacy Act (British Columbia), sections 42(1)(a) and 44.

“The present functions of the Commissioner should be maintained, with extension to others, such as audit, when resources are obtained.”

- ROYAL NZ COLLEGE OF
GENERAL PRACTITIONERS,
SUBMISSION G4

“Site visits have three primary goals:

1. To meet the head of the public body and the records and information management personnel;
2. To view how public body personnel collect, use, store, disseminate, and dispose of the personal information in their custody or under their control; and
3. To address any immediate concerns regarding the privacy, security, and accessibility of records held by the public body.

“The office can report that no public body visited so far has been in serious breach of the information practices required under the Act. However, where the Commissioner and/or his staff have uncovered specific concerns, the office has discussed those concerns with the public body immediately and conducted follow up activities to ensure compliance.

“Site visits have proven to be one of the most effective and immediate approaches to raising a public body’s awareness about its legislative obligation to handle records in accordance with requirements of the Act. This is especially important with respect to public bodies that collect and store highly sensitive and potentially stigmatising personal information.”¹⁹

- 3.3.22 Auditing has been used successfully by various commissioners, including the Australian Privacy Commissioner.²⁰ However, the experience, successful though it has been, of the commissioners in Australia and Canada does not necessarily directly translate into a suitable model for New Zealand given that, unlike theirs, my jurisdiction covers both public and private sectors.²¹ It is probably for this reason that function (b) is written so that audits may only be undertaken “when requested by an agency”. The consensual model has reassured people that a heavy handed commissioner will not unnecessarily get involved in the affairs of individual businesses. Instead, the Act anticipates that agencies themselves will request an audit²² or the Commissioner may ask an agency to agree to be audited. It may be useful to note the position in two jurisdictions in which the law covers the private sector.

UK and Hong Kong

- 3.3.23 The UK Data Protection Bill introduced into Parliament in early 1998 confers upon the Data Protection Commissioner a function very much like the one contained in the Privacy Act. Clause 49(5) states:

“The Commissioner may, with the consent of the data controller, assess any processing of personal data for the observance of good practice and shall inform the data controller of the results of the assessment.”

- 3.3.24 The Hong Kong law was preceded by a Law Reform Commission report which commented that on-site inspections:

“... are referred to in other countries as data protection ‘audits’ but, as that term might appear overly negative, we prefer

¹⁹ Office of the Information and Privacy Commissioner for British Columbia, *Annual Report 1996-97*, pages 98-99.

²⁰ Privacy Commissioner of Australia, *Ninth Annual Report*, 1996/97, 89-99, discusses the exercise of audit powers.

²¹ However, the Australian Commissioner *does* audit privacy sector credit reporting agencies.

²² None have yet done so.

‘verifications’. However described we consider them a vital function for an effective data protection body.”²³

- 3.3.25 The Law Reform Commission noted evidence received from the German Data Protection Authority. In Germany inspection teams attend sites for between 1 and 2 weeks, no disruption had been caused, or claimed to have been caused, to the activities of the inspected organisations.²⁴ The Law Reform Commission considered the audit power as applicable to the private sector and notes its application to the banking sector.
- 3.3.26 The Hong Kong Personal Data (Privacy) Ordinance includes an inspection power which does not distinguish between public and private sector agencies. It states:

“Inspections of personal data systems

Without prejudice to the generality of section 38 [which concerns investigations by the Commissioner on a complaint or where the Commissioner suspects a contravention], the Commissioner may carry out an inspection of:

- (a) any personal data system used by a data user; or
- (b) any personal data system used by a data user belonging to a class of data users,

for the purposes of ascertaining information to assist the Commissioner in making recommendations:

- (i) to:
 - (A) where paragraph (a) is applicable, the relevant data user;
 - (B) where paragraph (b) is applicable, the class of data users to which the relevant data user belongs; and
- (ii) relating to the promotion of compliance with the provisions of this ordinance, in particular the data protection principles, by the relevant data user, or the class of data users to which the relevant data user belongs, as the case may be.”²⁵

It is also too early to judge the operation of the Hong Kong provision since it has not been fully implemented yet. An inspection methodology is currently being developed.

NZ auditing

- 3.3.27 It is problematic that the New Zealand auditing power has not been able to be utilised and, on present indications, is unlikely to be. Problems include:
- I have no spare resources to devote to developing expertise and systems in this area of work;
 - while public sector agencies might be amenable to being audited, it may be difficult to obtain agreement that the cost fall entirely upon the agency being audited (the only practical option I have without annual resourcing to cover this function).
- 3.3.28 I am also concerned that independent auditing is not being used in areas where the public ought to be given an assurance that everything that is being undertaken in secret is “above board”. I have in mind the sort of audits formerly undertaken for the Wanganui Computer Centre Policy Committee and copied to the Wanganui Computer Centre Privacy Commissioner. Another example would be

²³ Law Reform Commission of Hong Kong, *Report on Reform of the Law Relating to the Protection of Personal Data*, 1994, paragraph 16.73.

²⁴ *Ibid*, paragraph 16.74.

²⁵ Personal Data (Privacy) Ordinance (Hong Kong), section 36.

compliance with conditions upon warrants to intercept private communications.²⁶

- 3.3.29 A change in the law to remove consent would send an unnecessarily worrying signal that I am intent upon forcing agencies to be audited which is *not* the case. Any Privacy Commissioner with legal powers to do so, undertakes only a tiny number of very carefully prioritised audits. The audits are usually done on the basis of policy and strategic considerations but an element of chance may also play a part in selection. The audits themselves are usually scheduled months in advance and notice given before arrival at any premises.
- 3.3.30 Although the potential of auditing to enhance privacy, and to ensure compliance with the Act, has not been able to be fulfilled I do not recommend a change to the Act at this stage to create mandatory powers of audit. Instead, I hope that it may be possible to explore various options for the undertaking of audits pursuant to existing provisions. For example, the undertaking of internal audits, the results of which are reported to me, has already been successfully incorporated into conditions on approvals in the information matching sphere.²⁷ If the funding can be arranged to enable the development of a methodology and expertise, and the undertaking of some audits, I will be in a better position to judge whether the present voluntary arrangements for audits are satisfactory. By the time of the next review of the operation of the Act, it will also be possible to look to the new Hong Kong and the UK experience. Experimentation with less rigorous models such as “site visits” or “on-site surgeries” to flush out, and advise on, problems, could also be explored.

Function (c): Monitoring use of unique identifiers

- 3.3.31 I have been given the function of monitoring the use of unique identifiers and to report to the Prime Minister on the results of such monitoring from time to time. I have not exercised that function formally as yet as other priorities have taken precedence. I have nonetheless kept an eye on a variety of unique identifier issues. For example, three of the codes of practice I have issued have addressed unique identifier issues.²⁸ Such issues have also been identified in reports on certain legislative initiatives.²⁹ Issues about the use of unique identifiers also arise in the context of information matching - with the starting presumption that unique identifiers are not permitted to be used.³⁰
- 3.3.32 It is desirable to retain this function since it may be necessary to monitor the position more closely in the future. I have, for example, had some unease in the last year or so over the possibility of the existing National Health Index number being used as the building block for a nationwide medical population register - a project which would carry significant privacy risks.³¹ I have also been concerned at the possibility of the new driver licence becoming a national unique identifier.³²

²⁶ I recommended that an audit function, modelled on Australian law, be established in respect of compliance with the requirements of laws governing the interception of private communications and the conditions imposed on warrants. See my report to the Minister of Justice on the Harassment and Criminal Associations Bill, Interception of private communications, April 1997.

²⁷ See approval by the Privacy Commissioner under rule 3(1) of the information matching rules, 25 June 1996, conditions 7 and 8. Internationally there has been considerable interest in internal audit. The Canadian Standards Association has developed a model privacy code and is seeking to implement a certification arrangement including, in larger organisations, appropriate forms of compliance audit. The International Standards Organisation has also been considering the matter in the context of a possible technical or management standard.

²⁸ Health Information Privacy Code 1994, Superannuation Schemes Unique Identifier Code 1995 and Justice Sector Unique Identifier Code 1998.

²⁹ See Report to the Minister of Justice on the Taxation (Remedial Provisions) Bill, August 1997.

³⁰ See information matching rule 2.

³¹ See Robert Stevens, *Medical Records Databases: Just what you need?*, report prepared for the Privacy Commissioner, April 1998.

³² See Report to the Minister of Justice on the Land Transport Bill: Photo ID Driver Licences, March 1998.

Function (d): Directories of personal information

3.3.33 I discuss the function of maintaining, and publishing, directories of personal information in relation to section 21 at paragraph 3.11.

Function (e): Monitoring compliance with public register principles

3.3.34 I have not, as yet, attempted to systematically monitor compliance with the public register privacy principles. However, I have been alive to public register issues in the carrying out of my other functions. For example, I took the opportunity of the Parliamentary inquiry following the 1996 general election to prepare a report in relation to one of the most significant public registers, the electoral roll.³³ In 1995 my staff undertook a small project asking the agencies maintaining public registers about the search references in use and for their views on the purpose for which the registers are maintained.³⁴

3.3.35 The present exercise has provided an opportunity to review the public register principles. In doing so, I have, as directed in section 13(1)(e), had particular regard to the Council of Europe Recommendations on Communication to Third Parties of Personal Data held by Public Bodies.

Function (f): Examination of proposed information matching provisions

3.3.36 Under (f) I have the function of examining any proposed legislation which provides for the collection or disclosure of personal information which may be used for the purposes of an information matching programme. Most of the existing programmes were authorised in 1991 and there was a lull for over three years before the next proposal came forward. Accordingly, it was in October 1995 that I first examined proposed new information matching legislation in the Electoral Reform Bill.³⁵

3.3.37 Information matching - or data matching as it is called overseas - is an application of computer technology which carries particular privacy risks. It therefore warrants careful scrutiny. The policy adopted in New Zealand involves the obtaining of legislative authority for government information matching programmes. On the introduction of the Privacy of Information Bill the Minister of Justice stated that:

“It is entirely proper that this be approved by Parliament and not authorised simply by Executive fiat”.³⁶

3.3.38 The legislative proposal is examined by the Privacy Commissioner pursuant to function (f) and judged by reference to six information matching guidelines.³⁷ Government processes leading up to the introduction of any bill also ensure scrutiny of a proposal in terms of the information matching guidelines.³⁸ The Bill is further studied by a select committee. The report of the Commissioner’s examination provides a scrutiny independent of the Executive and Legislature. It is, of course, open for Parliament to enact an information matching provision regardless of concerns that might be expressed in the report. A resulting information matching provision provides statutory authorisation for any match and this prevails over any inconsistency with the information privacy principles.³⁹

³³ See Report to the Minister of Justice in relation to the Electoral Act 1993, April 1997.

³⁴ Office of the Privacy Commissioner, *Public Register Search Reference Project*, 1995.

³⁵ See Report of the Privacy Commissioner to the Minister of Justice on the Electoral Reform Bill, Information Matching of Electoral and Immigration Information, October 1995.

³⁶ Hon Douglas Graham (Minister of Justice), Introduction of Privacy of Information Bill, NZPD (5 August 1991) 3850.

³⁷ Privacy Act, section 98.

³⁸ See *Cabinet Office Manual*, August 1996, Chapter 5, paragraph 5.26, 5.29 and 5.58 and Appendix 6, Standard Format for Legislation Submissions.

³⁹ Privacy Act, section 7.

- 3.3.39 The result is, so far as I am aware, a unique process for the authorisation of information matching although it draws upon features from the Australian experience. It brings together governmental, legislative and independent, scrutiny which results in a high level, and robust, authorisation for permitted programmes. It involves a very explicit examination, and balancing, of key features including the financial costs and benefits. Built into the process are checks to ensure that proper data protection practices will be observed.
- 3.3.40 I have now undertaken a number of examinations of proposed new information matching provisions.⁴⁰ In my first report I noted that there would be clear advantage in having a thorough analysis of the proposed information matching programme, couched in terms of the information matching guidelines, completed by the proposing department at an early stage, ideally preceding Cabinet approval. Accordingly I have required departments to submit to me an assessment of their proposed programme so as to enable the examination to be carried out. I issued a guidance note on preparing the information matching privacy impact assessment document (IMPIA).
- 3.3.41 I have found the legislation to be satisfactory in respect of examination of proposed information matching provisions although I suggest elsewhere several modest amendments to the information matching guidelines.⁴¹ The difficulties that I have encountered have not been with the legislation but with certain practical factors. Principal amongst these is timing. A recurrent experience has been that departments have given me the necessary information so late in the development of a proposal that I have had to conduct a hurried examination. This is particularly problematic when the IMPIA is supplied after the introduction of a bill into Parliament.
- 3.3.42 I see no need to amend the provision although I do intend to further refine the examination processes so that they identify the key issues in respect of a proposal at the earliest time and so that the IMPIA provides a helpful step towards compliance with the statutory requirements once the match is authorised.

Function (g): Educational programmes

- 3.3.43 Paragraph (g) provides that I have the function:

“for the purpose of promoting the protection of individual privacy, to undertake educational programmes on the Commissioner’s own behalf or in co-operation with other persons or authorities acting on behalf of the Commissioner”.

- 3.3.44 Clearly there is something of an overlap in this function with paragraph (a) which empowers me to promote, by education and publicity, an understanding and acceptance of the information privacy principles and the objects of those principles. The two aspects that I would stress for function (g) here are the nature of educational *programmes* and the aspect of *co-operation*.
- 3.3.45 An education *programme* suggests a series of events, actions or things which have continuing or repeated use. Without attempting a comprehensive survey of the last 5 years I offer the following illustrations of programmes carried out pursuant to this function:

Seminar series with NZ Law Society

With the coming into force of the Privacy Act I participated in a nationwide series of seminar/workshops run under the auspices of the NZ Law Society

⁴⁰ See Appendix F in which I list the reports submitted to the Minister of Justice. The full reports are reprinted in Office of the Privacy Commissioner, *Examination of Proposed Information Matching Programmes*, March 1998.

⁴¹ See recommendations 122, 123 and 124.

continuing legal education programme. The published seminar notes was a valuable resource in the first year of the Act when there was otherwise very little published on the Act of a substantial nature. In 1997 I participated in a follow-up NZLS seminar series. A useful resource book was published and is still available.

Seminar series with other organisations

On occasion, I have participated in series of seminars or workshops which are repeated in several locations around the country. One such initiative was run by a private trainer for the benefit of the health sector which I co-presented with the Health and Disability Commissioner. Another series of workshops was organised for senior journalists in conjunction with the Newspaper Publishers Association.

Seminars and workshops

From the outset my staff and I responded to numerous requests to speak to organisations. The office developed various formats for presentations. An overview seminar needed about 60 minutes with a more interactive workshop at least 90 minutes. Formats were developed for general and health sector audiences. Despite the positive feedback received from agencies for whom we conducted basic seminars, I was not convinced that this was the most efficient way to educate agencies about the legislation. Consequently, I launched a new training initiative which involved my office offering twice monthly half day workshops in Auckland and Wellington and, less frequently, in Christchurch. An introduction to the Privacy Act is repeated many times during the year as is a more advanced workshop. Supplementary modules target particular subjects, for example, employment or health issues. In-service workshops have also been conducted within agencies.

Videotape

In June 1995 I launched a professionally produced 27 minute videotape which was intended to increase awareness of privacy issues and to encourage agencies to consider the advantages of good personal information handling practices. *Mind Your Business* was prepared to such a high standard that it was accepted for broadcast by educational television twice on TV1. The videotape is accompanied by a trainers' booklet so that it may be used in in-house educational programmes and is occasionally used in conjunction with my office's own workshops. Copies are made available for purchase and on loan.

Private Lives? An Initial Investigation of Privacy and Disability Issues

In 1994 I republished an Australian publication on privacy and disability issues. I prepared an insert, specific to New Zealand and, with assistance and financial contributions from several public agencies, systematically distributed thousands of copies to all health and disability service providers in the country. Other activities were arranged in conjunction, including bringing the author of the report from Australia to the 1994 Privacy Issues Forum and enabling her also to speak to local health and disability sector groups. A special launch was organised by the Southern Regional Health Authority in Christchurch.

- 3.3.46 Submission G17 suggested splitting the educational function from the complaints function so as to have two separate entities performing the tasks. Change is not warranted. There already is a separate body which rules, in a binding sense, on complaints - the Complaints Review Tribunal. I find that the roles can be adequately combined and the educational function is enriched by experience of investigating real cases.

Function (h): Public statements

- 3.3.47 At first glance, the function of making public statements may seem rather unusual. In fact, similar provisions appear in comparable New Zealand legislation

“For our clients we would like to have available plain English pamphlets on the Privacy Act. Bureaux want more training on the Act and some bureaux have indicated the cost of the Privacy Commissioner’s Office training seminars was off putting for them as community groups.”

- NZ ASSOCIATION OF CITIZENS
ADVICE BUREAUX, SUBMISSION S26

such as the Human Rights Act⁴² and the Health and Disability Commissioner Act.⁴³ The function of independent Commissioners to make public statements in their various jurisdictions is an important one. The practice of speaking out publicly in order to promote, or protect, human rights is a common technique in all aspects of human rights work. In respect of information privacy issues it is especially useful to promote public awareness and discussion of privacy issues affecting individuals since frequently there is a limited level of understanding of the issues, particularly where they concern situations caused by new or converging technologies.

3.3.48 I have actively sought to promote public understanding, and awareness, of privacy issues through the release of public statements. I believe that privacy issues in the late 1990s require that approach to supplement any “behind the scenes” work for privacy or the necessarily confidential work involved in complaints investigation and settlement. Parliament in enacting the Act expects the Privacy Commissioner to publicly articulate important privacy concerns.

3.3.49 While I have used public statements in an effort to raise privacy concerns, or explain issues, most of the news media statements that I make are not initiated by me but in response to a journalist’s enquiry. Nonetheless, I resist many opportunities to make public statements through the news media due to the fact that I generally make no public statement on matters that are, or could be, the subject of a complaint to my office. Even when a complaint has been resolved it is not my usual practice to speak publicly on actual facts but instead, where warranted, issue a case note in which the complainant is anonymised.

Function (i): Representations from the public

3.3.50 One of my functions is to receive and invite representations from members of the public on any matter affecting the privacy of individuals. I frequently *receive* unsolicited comments from the public and this has been a valuable input into my work. I have been pleased that so many members of the public have shown an interest in privacy. Sometimes I can act upon representations from the public to provide practical and effective input into public policy processes in a way that an individual citizen cannot.

3.3.51 The second part of the function is to *invite* representations. Generally I have done this in an informal manner by indicating in public statements and in correspondence that I am always open to receive representations on matters affecting privacy or concerning the operation of the Act. On occasion I have more formally sought representations. For instance, in relation to this review exercise I placed public notices and otherwise solicited representations from members of the public. I have also done so on particular issues on which I wish to hear from affected individuals. For example, as a precursor to preparing a report in relation to the mandatory publication of remuneration details under the Companies Act I made a public statement inviting executives with views to make representations to me.⁴⁴ I have from time to time invited representations on the Health Information Privacy Code and, in particular, on rule 11.

Function (j): Co-operation with others concerned with privacy

3.3.52 It has been a matter of disappointment to me that since the demise of the Privacy Foundation with the introduction of the Privacy of Information Bill there has been no organised group of citizens involving itself in privacy issues on a regular basis. Privacy advocacy groups in other countries actively promote a privacy viewpoint.

⁴² Human Rights Act 1993, section 5(1)(l).

⁴³ Health and Disability Commissioner Act 1994, section 14(1)(d).

⁴⁴ See Report of the Privacy Commissioner to the Minister of Justice, Disclosure of Executive Remuneration under section 211 of the Companies Act, November 1997.

“Too often the Commissioner does not comment because the issue in question might be raised in a subsequent case. The Federation has long been concerned about the roles of education and enforcement lying with the same people.”

- NZ EMPLOYERS

FEDERATION INC, SUBMISSION G10

3.3.53 I have been pleased to co-operate with other bodies where they have, for example, organised seminars, written leaflets or booklets on privacy, and such like. I have also co-operated with officials with privacy amongst their responsibilities. For example, my office has good working relations with the Ministry of Justice and the Ombudsmen's Office. I have also been pleased to co-operate with complaints bodies such as the Banking Ombudsman and the Insurance and Savings Ombudsman to the benefit of our mutual complainants and respondents. Elsewhere I have mentioned co-operation with such bodies as the Law Society and Mental Health Commission in various activities.

Regional co-operation

3.3.54 In other jurisdictions there are Commissioners and Commissions carrying out very much the same work as I do. The co-operation I have had from other Commissioners has significantly helped me in the carrying out of my functions. As my office has become more experienced, I have been pleased to say that the sharing of experience has been reciprocated.

3.3.55 In this regard, I particularly wish to acknowledge the co-operation of Kevin O'Connor, the former Australian Privacy Commissioner. The assistance extended, ever since the Privacy Commissioner Act 1991, has been invaluable and included, from the early months of my appointment, the making available of a senior staff member to advise on the Privacy of Information Bill and extended to an invitation to participate in the National Privacy Agencies meeting held with the various State bodies having a role in the protection of privacy. That 6-monthly meeting was later renamed the Privacy Agencies of New Zealand and Australia (PANZA) and has developed as a valuable forum for information exchange, consultation and co-operation. Its regional significance has grown in recent times with the participation of the Hong Kong Privacy Commissioner for Personal Data. I am pleased to say that co-operation with Kevin O'Connor's successor, Moira Scollay, has continued to be valuable for my office.

3.3.56 There are a limited number of specialist privacy organisations in our region. As well as the Australian and Hong Kong Commissioners, the PANZA meeting has facilitated co-operation with the New South Wales Privacy Committee and the South Australia Privacy Committee. It has also been valuable, through that forum, to establish networks on particular projects with the Australian Attorney General's Department, various officials in States Attornies' offices and others such as the Western Australian Information Commissioner.

3.3.57 The EU Directive on Data Protection has brought new attention to the adequacy of privacy laws. There are at present few comprehensive data protection or privacy laws in our region, with the Hong Kong Ordinance and the New Zealand Act the prime examples. Australia's Privacy Act applies primarily to the Commonwealth public sector and credit reporting agencies, leaving the State public sector and private sector without privacy law coverage. There are also laws in Japan, South Korea and Taiwan although their coverage tends only to be the public sector or automatically processed data. Interest has been shown in privacy laws by Malaysia and Singapore because of their trading relationships. There are currently no privacy laws in Pacific Island countries.

3.3.58 Something of a regional dialogue amongst agencies having responsibility for aspects of information privacy has commenced in recent years with a first tentative Pan-Pacific meeting in Victoria BC in 1996 and a more fully representative First Asia Pacific Forum on Privacy and Personal Data Protection in Hong Kong in April 1998. In 1997 I included on the agenda of the PANZA meeting I hosted in Auckland the question of privacy protection in the Asia-Pacific and was pleased, with assistance from the Ministry of Foreign Affairs and Trade, to be able to invite representatives from Western Samoa, Papua New Guinea, In-



Bruce Slane and Kevin O'Connor: The New Zealand and Australian Commissioners confer at the 1996 Privacy Issues Forum.

PHOTO: OFFICE OF THE PRIVACY COMMISSIONER

dia and the Philippines. I have, for some time, been concerned that the debate about the implications of the EU Directive on third countries ignores the position of developing countries. The issues are now getting a wider airing.

International co-operation

- 3.3.59 It has also been valuable to meet with Privacy and Data Protection Commissioners from a variety of other jurisdictions in the annual International Conference of Privacy and Data Protection Commissioners. There are more than 40 such commissioners and the number grows with each conference, particularly as the former Eastern bloc has embraced human rights and nations respond to the implications of the European Union Directive on Data Protection. I have contributed to such conferences and established valuable contacts with commissioners struggling with the same vexed privacy issues that I do. The approach of Privacy Commissioners internationally is similar on most privacy issues even though the techniques applied, and the detail of the legislation under which they operate, may differ. This is because the OECD Guidelines and the European instruments provide a clear and consistent set of international principles governing data protection and fair information practice.



International cooperation:
Delegates to the 23rd Meeting
of the International Working
Group on Data Protection in
Telecommunications,
April 1998.
PHOTO: HONG KONG
PRIVACY COMMISSIONER FOR
PERSONAL DATA

- 3.3.60 Now that privacy laws are the norm in countries of our type, the size of the international conference has grown quite large. Accordingly, I took the initiative at the conference in 1996 to convene in conjunction with the conference a small workshop of commissioners in a committee room of the Canadian Parliament. The workshop sought to address the “how to” aspects of achieving effective education and publicity activities and providing input into legislative processes. It was well received with participation from Canada, Germany, Hong Kong, The Netherlands and the British Isles.

Other co-operation

- 3.3.61 It is not possible to list all the types of co-operation undertaken with others concerned with privacy. Co-operative initiatives range from the tiny to the moderately extensive. Two initiatives may suffice to illustrate:
- I have developed an extensive specialist collection of publications on privacy issues. On occasion I receive duplicate reports and have entered into an arrangement to deposit some of these with the Davis Law Library at the University of Auckland.
 - Recently an organisation associated with Alan Westin, well known American author and researcher on privacy issues, has developed an Internet site from which it is hoped to disseminate key data protection documentation. This includes links to laws and websites around the world and I have agreed to allow my own site to be hyperlinked.⁴⁵

Function (k): Suggestions for action

- 3.3.62 I, and my office, are constantly making suggestions to various people concerning the need for, or the desirability of, action in the interests of privacy of the individual. Although I do not have all the answers I have endeavoured to have my office offer constructive suggestions, and occasionally solutions, to privacy problems rather than simply to criticise the actions of others. Where agencies

⁴⁵ www.PrivacyExchange.org

have been open to constructive criticism, and suggestions for alternative actions, I have usually found that information privacy problems are well capable of practical and cost effective solutions.

Function (l): Advice to Ministers or agencies

3.3.63 I have the function “to provide advice (with or without a request) to a Minister or an agency on any matter relevant to the operation of the Act.” Most of the advice offered is in response to a request. Occasionally, I offer unsolicited advice and frequently that is welcomed as enabling an agency to avoid a compliance problem. Of course, sometimes advice which has not been asked for is not welcomed. As a watchdog on privacy issues I can be the bearer of unwelcome news on occasion. I accept any lack of appreciation for such advice as part of the job.

3.3.64 My advice is contestable since I have few powers to prohibit action or issue rulings. Ministers and others are free to disregard my advice or to seek another opinion elsewhere. However, the importance of the express function is that it makes quite clear that I have a proper role in offering advice even where that has not been requested. The absence of such a function in other jurisdictions has sometimes resulted in suggestions that a Privacy Commissioner has no place in becoming involved in an issue unless he or she has been formally consulted. This is not the position in New Zealand. The Privacy Commissioner is clearly given a roving brief to offer advice on privacy issues whether privately or publicly, asked or unasked. If an independent Commissioner is to fulfil his or her task nothing less is warranted. Ministers and others are free to criticise the advice that I offer or suggest that I am wrong, but there is no place for saying the Commissioner should not offer advice on matters relevant to the operation of the Act.

Function (m): Inquiry into enactments, practices, procedures, technical developments etc

3.3.65 This function can be looked at in two ways. If one considers “inquire into” in an informal and general sense then it is a function that is frequently undertaken and is a staple part of the work that my office does. Considerable amount of activity is undertaken to seek information relating to laws, practices and technical developments, which may infringe privacy so that they are better understood, problems can be avoided, and matters can generally be influenced in some way to better protect privacy.

3.3.66 However, if the function is seen as having a more formal application then it is not yet one that I have exercised. The function, would, it appears, empower me to convene a formal inquiry into any matter where it appears that the privacy of an individual is being, or may be, infringed. An example of that kind can be found in the New South Wales Privacy Committee’s recent inquiry into covert video surveillance in the workplace which was the first such formal inquiry since its establishment in 1975.⁴⁶ It may well be appropriate to undertake such inquiries from time to time although they will, of course, involve the commitment of a considerable resource and therefore have to carefully compete with other priorities.

3.3.67 I take the view that this function encompasses both the informal activity described above and also formal inquiries. Whichever interpretation is placed upon it the function is a usual one for a Privacy Commissioner and a necessary one to retain.

Function (n): Research and monitor data processing and computer technology

3.3.68 The function to research into, and monitor developments in, data processing and computer technology to ensure that any adverse effects of such developments on the privacy of individuals are minimised, and to report to the Minister the results

⁴⁶ The inquiry was undertaken pursuant to section 15(1) of the Privacy Committee Act 1975. Formal terms of reference were announced, submissions taken, and the resultant 132 page report published as: Privacy Committee of New South Wales, *Invisible Eyes: Report on Video Surveillance in the Workplace*, September 1995.

“The Federation does not consider that advance rulings would help reduce compliance costs, particularly as they would introduce an element of inflexibility while at the same time inevitably failing to cover new fact situations. The relatively non-prescriptive nature of the statute is one of its better features. Guidelines are, however, another matter and should be provided wherever possible.”

- NZ EMPLOYERS FEDERATION,
SUBMISSION WX3

of such research and monitoring, is an important one. I would like to be able to undertake more work in that area. Activity by overseas Commissioners has led to a variety of valuable reports and resultant action. The Commissioners in Canada, Ontario, The Netherlands and Australia have an excellent reputation in this regard and reports of interest are starting to appear from the newer offices in British Columbia and Hong Kong. The Berlin Commissioner is active in coordinating research in relation to telecommunications and privacy issues.

3.3.69 Were I to undertake such research I would have careful regard to the work being carried on by colleagues in other jurisdictions so as to avoid duplication. The possibility of joint research with another Commissioner would offer potential to reduce the cost of such research or to enable more extensive projects than might be attempted alone.

3.3.70 In 1998 I commissioned some research into medical record databases and forwarded the resultant report to the Ministers of Justice and Health. I earlier commissioned research into aspects of drug testing and brought the researcher, Eugene Oscapella of Canada, to New Zealand to speak to the Privacy Issues Forum in Wellington and to employer and union groups. Although I have not formally reported to the Minister of Justice on that or other such projects I have nonetheless been active in researching, and informally monitoring, such issues for my own information in carrying out my functions. Participation in the annual Commissioners' conference, and PANZA meetings, have been valuable in monitoring developments.

Function (o): Examination of proposed legislation

3.3.71 I have the function of examining proposed legislation, including subordinate legislation, which may affect the privacy of individuals and to report the results of my examination to the Minister of Justice. Appendix F lists the reports I have submitted since 1992. Reports are available to the public shortly after the Minister has received and had a chance to consider them. Frequently the reports concern proposed legislation before a select committee and are followed up with an appearance before a select committee.

3.3.72 The *Cabinet Office Manual* requires departments to signify compliance with the information matching principles, public register privacy principles, and the information matching guidelines, when seeking introduction of a bill into Parliament or when proposing the issue of regulation. Accordingly, I have frequently been consulted by departments concerning new legislative proposals.

3.3.73 I have placed a considerable emphasis on exercising this function to provide a privacy input into the legislative process. There are a variety of reasons for this including:

- there has been since 1993 a series of legislative initiatives having considerable significance for privacy issues - such as the creation of a DNA databank, the enhancement of oversight controls on intelligence organisations, and the establishment of a photo ID drivers licence, to name three;
- by virtue of section 7 the requirements of enactments override the privacy principles and therefore it is important that the opportunity be taken to provide privacy input into the enactment of new laws and the review of existing ones;
- legislation often provide an opportunity for public education and the increase in knowledge about privacy issues amongst legislators and others - I do not simply oppose legislation but often seek to explain laws in privacy terms or support certain initiatives.

3.3.74 My office may be more active than some other Privacy Commissioners' offices in scrutinising legislative proposals and providing formal written reports which are made public. Part of this is simply a matter of priorities for my office compared with others. However, it is partly to do with the nature of lawmak-

“The Commissioner must be properly resourced so that complaint investigations can normally be completed within a month or an early date fixed for complex cases, and to be able to comment on all proposed relevant government policies, legislation or regulation.”

- AUCKLAND DISTRICT
COUNCIL OF SOCIAL SERVICE,
SUBMISSION G6

ing in New Zealand. There is often an openness and responsiveness amongst New Zealand officials and lawmakers to a well reasoned case whether it is on the grounds of privacy or any other. In those reports which have been copied to select committees, I have been pleased at the genuine interest shown in the issues by MPs and their willingness, when a problem has been established, to respond in the drafting of new laws. Such responsiveness does not always exist in large countries or in federal systems where lawmaking is more fragmented.

Function (p): Report to Prime Minister on need for action

3.3.75 During the period under review I made no reports to the Prime Minister on the need for any special action. However, I see the provision is valuable and would intend to use it on appropriate occasions especially where issues raised seem to have a wider or more general impact deserving attention by the Prime Minister rather than the Minister of Justice. The provision serves to underline my role independent of a Minister or ministry and it is appropriate to have this access.

Function (q): Report to PM on acceptance of international instrument

3.3.76 During the period under review I have not reported to the Prime Minister on the desirability of the acceptance by New Zealand of any instrument relating to the privacy of the individual. Much of the international work in the last couple of years has been in developing international instruments that require no national acceptance. For example, there has been work by the OECD in the areas of security of information systems and cryptography policy and the ILO has developed a code of practice on the protection of worker's personal data.⁴⁷ However, none of these are treaties to which countries can sign but instead have the status of guidelines. The European Union Directive on data protection, issued during the period, is not an international instrument that New Zealand can become a party to.

3.3.77 As far as I am aware, the only outstanding international instrument having general applicability to data protection and information privacy issues that New Zealand could accede to is the 1981 Council of Europe Convention No. 108. Although article 23 of that convention permits non-member states to accede none have done so. Most of the countries outside Europe which might have contemplated acceding have found the OECD Guidelines more appropriate as a basis for action. Interest may be rekindled amongst non-member states in acceding to the Convention as a means to encourage the EU to use this as a basis to judge the position in such a country as "adequate" in terms of the EU Directive.⁴⁸

3.3.78 I have not formally, or systematically, scrutinised Convention No. 108 with a view to judging whether New Zealand would be in a position to accede to it or to identify the benefits of doing so. Tentatively, I would see some problems in acceding when our law is modelled on the OECD Guidelines and omits some features anticipated in the Convention such as special controls on the processing of "sensitive data". Also the Convention is now quite old and no longer considered "state of the art". It is unlikely that New Zealand's position with regards to "adequacy" in EU eyes would need to be enhanced by accession to the Convention which otherwise would be the main benefit in accession.

Function (r): Report to PM on any other matter

3.3.79 During the period under review I have not had cause to report to the Prime Minister pursuant to this function. There is no need for amendment of the provision.

⁴⁷ International Labour Office, Code of Practice on the Protection of Workers' Data, November 1996.

⁴⁸ Countries which accede to Convention No. 108 and which have appropriate institutional mechanisms, such as an independent supervisory authority with powers, are thought likely to meet the adequacy test where the country is the final destination - and not an intermediary - of the data. See EC (DGXV), Working Party on the Protection of Individuals with regard to the Processing of Personal Data, "First orientations on Transfers of Personal Data to Third Countries - Possible Ways Forward in Assessing Adequacy," June 1997.

“The functions of the Commissioner could be usefully pivotal to the processes used by decision-makers in balancing competing interests under the Act. As it stands they are rather buried in section 13 and are not an obvious reference point for those using the Act.”

NZ LAW SOCIETY PRIVACY WORKING
GROUP, SUBMISSION G22

Function (s): Gathering information

3.3.80 It is apparent that many privacy issues revolve around the development of new technologies and the convergence of existing technologies. The pace of change has been rapid and it has been necessary to develop means of keeping my office informed of these “cutting edge” issues as well as the regular diet of important, and interesting, mainstream privacy issues. I have established within my office a specialist collection of privacy texts, journals and materials which has expanded rapidly and covers a wide variety of issues.

3.3.81 People working in the field of privacy are a valuable source of information. In addition to networks amongst overseas commissioners and experts I have established contacts within New Zealand amongst experts, officials and others working in the field. Perhaps one of the most useful networks has been the office’s contacts with privacy officers throughout government and business. These people are not necessarily “experts” in any formal sense but they possess a wealth of experience and I have frequently valued their insights.

Function (t): Incidental or conducive functions

3.3.82 It is quite usual to include in a list of functions a provision referring to anything incidental or conducive to the performance of any of the preceding functions. It is a necessary provision and need not be amended.

Function (u): Other enactments

3.3.83 Function (u) at first appears similar to the previous function in being a “catch-all” or “tidy-up” provision. However, it is more than this. By virtue of the existence of a Privacy Commissioner, with an office having facilities for complaints investigation and resolution, public education, research and other activities, it is open to Parliament to confer tasks upon the Commissioner in other laws without the need to establish any new institutions or enact elaborate legislative machinery.

3.3.84 It can be convenient for a Government, or Parliament, to confer functions upon the Privacy Commissioner in another law for several reasons. For example, a proposal contained in that law might raise public concerns. Without abandoning the basic proposal, the conferring of a special “watchdog” role upon the Commissioner may allay public concern and allow the proposal to proceed. Typically, this might involve requiring a public agency to consult with the Privacy Commissioner in the implementation of a new scheme. A complaints role might be conferred upon the Commissioner in anticipation of exceptional circumstances if there is a worry that new powers might be used in an unexpected way or that something might go wrong. Placing a complaints function with the Commissioner is cheaper than creating a special new procedure, or complaints body, especially where complaints are expected to arise only rarely.

3.3.85 Appendix G summarises most of the existing functions conferred upon the Commissioner by other statutes. Some, particularly those involving consultation on the implementation of a new programme, happen once and the Commissioner may have little or no continuing involvement with the issue. Others, such as new complaints processes, sometimes give the Commissioner an ongoing, albeit usually infrequent, role.

3.3.86 In Appendix G the functions conferred on the Commissioner to date are set out in six categories:

- complaints mechanisms;
- Commissioner’s approval;
- consultation;
- appointment to another body;
- codes of practice;
- information matching.

Complaints mechanisms

3.3.87 Few complaints have been received under the complaints functions established under the Health Act, Domestic Violence Act and Social Security Act.

Approval of, and consultation with, Commissioner

3.3.88 The Passports Act 1992 contains two provisions which appear on their face to contain a strong privacy safeguard. They require the Commissioner's *approval* before certain disclosures can be made out of New Zealand. These are the only such provisions as it has usually been considered satisfactory in other cases to simply provide for consultation with the Commissioner. The requirement for approval is perhaps explained by the fact that the provision was enacted before the full Privacy Act 1993 framework was in force. The other consultation provisions vary in their implications for the Office. Consultations under the Official Information Act and Local Government Official Information and Meetings Act involve a significant call on resources. The other consultations tend to be infrequent and not particularly time consuming.

Appointment to other bodies

3.3.89 I am designated as a Human Rights Commissioner under the Human Rights Act 1993 by virtue of my appointment. This is the only such appointment. I would not favour any general practice of appointment to other bodies and committees. I am aware that in other jurisdictions Commissioners sometimes do accept such appointments but I presently take the view that it usually provides for better use of my resources for other statutory entities to consult with me where relevant rather than being appointed to another body.

3.3.90 Section 7 of the Human Rights Act 1993 provides that the Privacy Commissioner is a member of the Human Rights Commission. Prior to 1993 the Human Rights Commission itself had a “watching brief” on privacy issues. The Ombudsman was formerly a member of the Human Rights Commission but generally did not attend meetings. Neither the Commissioner for Children (established in 1989) nor the Health and Disability Commissioner (established in 1994) were added to the membership of the Commission when those positions were created.

3.3.91 Membership of the Human Rights Commission does involve spending time away from privacy work. The main commitment involves approximately 10 full day Commission meetings each year with additional preparation time. On one occasion I acted as alternate Proceedings Commissioner on a Human Rights Act case where the Proceedings Commissioner himself was unable to act, involving a further sustained commitment of time.

3.3.92 The discussion paper asked whether the Privacy Commissioner should continue to be a member of the Human Rights Commission. Only 9 responses were received with 6 supporting continuation of the present position,⁴⁹ 2 neutral⁵⁰ and one opposed to the Commissioner continuing on the Commission.⁵¹

Codes of practice and information matching

3.3.93 Other statutes have sometimes supplemented my powers and functions with respect to codes of practice, and information matching (see Appendix G). In respect of codes, the provisions have usually empowered the Commissioner to do some precise thing relevant to the other law by way of code of practice. In the information matching field, it is sometimes provided that a provision that is not an information matching provision is to be monitored as if it were.

⁴⁹ Submissions M3, M4, M7, M10, S4 and S42.

⁵⁰ Submissions M16 and M17.

⁵¹ Submission S3.

Subsection (2)

- 3.3.94 Subsection (2) provides authority for me to publish reports whether or not the matters have been the subject of a report to the Minister of Justice or the Prime Minister. For example, I am empowered to publish notes of cases that I have investigated and have done so, usually anonymising the material sufficiently that the complainant, and often the respondent, cannot be identified. I believe the publication of reports is an important part of my job to disseminate appropriate information both for public education and to assist agencies in compliance with the law.

3.4 SECTION 14 - Commissioner to have regard to certain matters

- 3.4.1 Section 14 is an important provision although it is often overlooked by critics at the legislation. For this reason I set it out in full:

“Commissioner to have regard to certain matters - In the performance of his or her functions, and the exercise of his or her powers, under this Act, the Commissioner shall:

- (a) Have due regard for the protection of important human rights and social interests that compete with privacy, including the general desirability of a free flow of information and the recognition of the right of government and business to achieve their objectives in an efficient way; and
- (b) Take account of international obligations accepted by New Zealand, including those concerning the international technology of communications; and
- (c) Consider any developing general international guidelines relevant to the better protection of individual privacy; and
- (d) Have due regard to the information privacy principles and the public register privacy principles.”

- 3.4.2 Paragraphs (c) and (d) tend to guide me as to what meaning I should give to notions of privacy. I am guided by the information privacy principles and public register privacy principles in the main. However, where there are international guidelines relevant to the protection of privacy this also gives me a steer so that my approach and interpretations are informed by, and remain consistent with, the international approach to privacy. Paragraph (b) also gives some guidance on privacy but it is sometimes the case that international obligations *compete* with privacy.

- 3.4.3 However, it is paragraph (a) that is probably of most interest and important when considering section 14. I am required to have regard for certain interests that compete with privacy. Indeed, this is an everyday part of being a Privacy Commissioner. Section 14(a) makes explicit what would otherwise likely be an implicit part of the job in any case. It involves the balancing of privacy against competing interests since there is no notion of an absolute state of perfect privacy and instead there is something of a continuum depending on the degree to which an individual interacts with society and is able, or must surrender autonomy.

- 3.4.4 Often section 14 considerations are so much integrated into my approach to issues, or the work of my office, that they are not explicitly referred to. For example, seeking to reach a settlement on a complaint will often involve considering the needs of Government and business to achieve their objectives in an efficient way in order to give meaning to the various exceptions to the privacy principles or the “reasonableness” tests that appear in many of them. Aspects of section 14 are also a consideration for me in other functions such as in deciding

“The NZBR welcomes the wide definition of ‘compliance cost’, including opportunity costs, adopted by the Commissioner. However, we note that the Commissioner defines costs as excessive only if it would be practicable to achieve the essential objects of the legislation without all or some of the actual costs being incurred. In other words the principles of the Act are taken as given and are not themselves to be subjected to any cost/benefit analysis. The NZBR considers that the concept of the Act should itself be subject to review.”

- NZ BUSINESS ROUNDTABLE,
SUBMISSION S50

whether or not to proceed with a code of practice and in reporting to the Minister on a legislative proposal.⁵² Section 14 is derived from a similar provision in the Australian Privacy Act.⁵³

- 3.4.5 The provision is drafted in such a way that it takes account of the changing international landscape without the need for any particular amendment. For example, the OECD has issued two recent sets of guidelines, and is considering another, which are automatically, through the operation of section 14, a consideration for the Commissioner.⁵⁴ The European Union Directive is having a great deal of influence internationally and is referred to at many parts of this report.
- 3.4.6 It may be worth observing that, while I am directed to have regard to the provisions in section 14, no such obligation exists upon agencies or the Complaints Review Tribunal.⁵⁵ This is appropriate, in my view, on both accounts. There is little point in directing agencies to have regard to certain matters of the type set out in section 14 and it would be unrealistic and meddlesome to do so. Less clear cut is the position of the Tribunal. However, to give directions to a court or tribunal to have regard to the sort of matters provided for in section 14 would insert an undesirable degree of uncertainty into proceedings for little benefit.

3.5 SECTION 15 - Deputy Commissioner

- 3.5.1 Section 15 provides for the appointment of a Deputy Privacy Commissioner. Under the control of the Commissioner, any deputy would have all the powers, duties and functions of the Commissioner, other than as a member the Human Rights Commission. A deputy would also act whenever the Commissioner's office falls vacant or when the Commissioner is absent from duty. No deputy has been appointed to date.
- 3.5.2 The section concerns a deputy appointed by the Governor-General on the recommendation of the Minister of Justice and not, as happens in some jurisdictions, an Assistant or Deputy Commissioner recruited by the Privacy Commissioner to take on certain functions delegated specifically by the Commissioner. The provision is similar to that provided in the Police Complaints Authority Act 1988⁵⁶ and the Health and Disability Commissioner Act 1994.⁵⁷ The approach taken in these three statutes differs from that in the Ombudsmen Act 1975 which provides for the appointment of more than one Ombudsmen, one of whom is the Chief Ombudsman.⁵⁸
- 3.5.3 The provision for a Commissioner and a deputy is an attempt to capitalise upon the strengths of a single person "Commissioner" model while addressing its principal shortcomings. For example, the deputy can share the workload and act where the Commissioner is incapacitated. A deputy could offer continuity in any transition. However, some of the advantages of a deputy can, in any case, be achieved through the delegation of certain functions to senior staff. I already delegate some functions.
- 3.5.4 Subsection (3) provides that a deputy Commissioner may not exercise the function of being a member of the Human Rights Commission. There may be

⁵² For example, in my report to the Minister of Justice on the Trans-Tasman Mutual Recognition Bill, April 1997. I explicitly noted that I had considered the international obligations undertaken by New Zealand.

⁵³ Privacy Act 1988 (Australia), section 29.

⁵⁴ The OECD issued its guidelines on information security in 1992 and five years later issued guidelines on cryptography policy. Guidelines are in preparation on consumer protection in electronic commerce.

⁵⁵ Or indeed the courts, which can adjudicate on certain access and correction proceedings - see section 11(1).

⁵⁶ See section 8.

⁵⁷ See section 9.

⁵⁸ See Ombudsmen Act 1975, section 3.

III

s 15

131

“The Ministry has in the past undertaken some work concerning compliance costs and the Privacy Act. Our conclusion drawn from these experiences is that while at an anecdotal level there are assertions of burdensome compliance costs, few organisations are able to substantiate these claims with concrete evidence that the Privacy Act imposes long term compliance costs, beyond that expected from appropriately targeted regulation.”

- MINISTRY OF JUSTICE,
SUBMISSION WX11

instances where a deputy brings with him or her superb qualifications for contributing to the Human Rights Commission and where it would suit the Privacy Commissioner, on occasion or generally, for the deputy to do so. It seems to me that the constraint in subsection (3) limits the possibilities for best use of a deputy. It is not clear that the restriction would prevent a deputy being involved in the work of the Human Rights Commission by virtue of appointment as an alternate under section 8 of the Human Rights Act. This ought to be clarified.



RECOMMENDATION 38

Section 15(3) should be amended to make clear that a deputy may be designated as an alternate Human Rights Commissioner with the concurrence with the Chief Human Rights Commissioner.

3.6 SECTION 16 - Term of office

- 3.6.1 It is essential for a Privacy Commissioner's independence to be guaranteed through the statutory appointment and removal provisions and through the term of office. An unduly short term of office, with frequent renewals, could give rise to public suspicion that a Commissioner would defer to the government for fear of risking non-appointment or that a government could use the actual or implied threat of non-reappointment to seek to control the Commissioner. Some jurisdictions resolve the issue by providing for a single, relatively lengthy, term of office which is not open to renewal.⁵⁹ The current New Zealand practice with most such appointments is to provide for a five year term with provision for renewals.
- 3.6.2 The Act provides that the Commissioner's term of office is for a maximum of five years. Such appointments are renewable. I was appointed pursuant to section 4 of the Privacy Commissioner Act 1991 for a term of five years. My term of office was continued when the Privacy Act 1993 consolidated the 1991 Act.⁶⁰ In 1997 I was reappointed for a further term of three years.
- 3.6.3 I believe that the term provided for in section 16, and the provision for reappointment, are satisfactory. The provision relating to the term of office is the same as provided for in the Privacy Commissioner Act 1991⁶¹ and for similarly situated Commissioners such as, the Health and Disability Commissioner.⁶²

3.7 SECTION 17 - Continuation in office after term expires

- 3.7.1 The Act provides that where a Commissioner's term of office expires, the occupier may continue in office until further provision is made for reappointment, succession, or vacation of office. This follows the same provision made in the Privacy Commissioner Act 1991.⁶³ Similar provision appears in other statutes establishing independent Commissioners.⁶⁴
- 3.7.2 The provision addresses a real issue, the need for continuity where a term of appointment comes to an end and a new appointment, or a reappointment, has not been finalised. However, therein lies a matter of concern. Where a Commissioner's own term of office has expired and a continuation in office occurs solely by virtue of section 17, there exists a situation whereby the independence

⁵⁹ In British Columbia the Commissioner holds office for a term of 6 years but is not eligible for reappointment. See Freedom of Information and Protection of Privacy Act (British Columbia), section 37.

⁶⁰ See section 133 of the Act.

⁶¹ See section 9.

⁶² See Health and Disability Commissioner Act 1994, section 12.

⁶³ See section 9(3).

⁶⁴ See, for example, Health and Disability Commissioner Act 1994, section 12(3).

of the office could be impugned. In such circumstances, a Commissioner's independence is not protected by a fixed term in office. I am aware of examples in New Zealand and elsewhere where similarly placed Commissioners have approached, or even gone beyond the expiry of their term of office, not knowing whether and when a further appointment, or a reappointment, is to be made. Such a position undermines the credibility of the appointment processes and the independence of the relevant offices.

- 3.7.3 Ministers, and particularly the officials who advise them, must not rely on provisions such as section 17 to allow delay to creep into the taking of decisions on appointments or reappointments which must, at some stage, be taken. Section 17 is an appropriate provision to utilise where an appointment of a new Commissioner has been made and the existing Commissioner remains in office for the convenience of the change-over. It is also an appropriate provision to allow, for a matter of weeks not months, the reappointment processes to be completed where Ministers make their intentions known to a Commissioner. However, it would be improper, in my view, for a government to allow the position to drift for a matter of months following the completion of a term through reliance upon the section. Care should be taken to ensure that this does not happen.

3.8 SECTION 18 - Vacation of office

- 3.8.1 Section 18 provides for the removal and resignation of the Privacy Commissioner from office. Special provision is made for when a judge is appointed as a Commissioner. To preserve the independence of the office, the Commissioner cannot be removed during a term of office except by the Governor-General on the recommendation of the Minister for:
- inability to perform the duties of the office;
 - bankruptcy;
 - neglect of duty; or
 - misconduct.

- 3.8.2 This provision is appropriate and reflects similar provisions in the Privacy Commissioner Act 1991⁶⁵ and in statutes establishing other Commissioners.⁶⁶

3.9 SECTION 19 - Holding of other offices

- 3.9.1 Section 19 restricts the Privacy Commissioner holding other offices. The Commissioner is not permitted to be a member of Parliament or of a local authority. The Commissioner is not permitted to hold any office of trust or profit or engage in any occupation for reward outside the duties of the Commissioner's office except with the approval of the responsible Minister in each particular case. It is an appropriate restraint.

3.10 SECTION 20 - Powers relating to declaratory judgments

- 3.10.1 Section 20 deals with the obtaining of declaratory judgments by the Privacy Commissioner. The process involves me referring a matter to the Proceedings Commissioner. I have not exercised the power during the period under review although I have on occasion considered whether it might usefully be applied to clarify an issue.
- 3.10.2 The only minor change that ought to be made to the provision is to replace the reference in subsection (2) to the Human Rights Commission Act 1977 with a reference to the Human Rights Act 1993.

⁶⁵ See section 11.

⁶⁶ See, for example, Health and Disability Commissioner Act 1994, section 13.

**RECOMMENDATION 39**

Section 20(2) should be amended by substituting “Human Rights Act 1993” for the reference to the “Human Rights Commission Act 1977”.

3.11 SECTION 21 - Directories of personal information

- 3.11.1 I am empowered under section 21 to publish, from time to time, a directory of information including some or all of the following:
- the nature of any personal information held by an agency;
 - the purpose for which any personal information is held by an agency;
 - the classes of individuals about whom personal information is held by any agency;
 - the period for which any type of personal information is held by any agency;
 - the individuals who are entitled to have access to any person information held by an agency, and the conditions under which they are entitled to have that access;
 - the steps that should be taken by any individual wishing to obtain access to any personal information held by any agency.
- 3.11.2 The objective of the directory is partly discerned from subsection 21(3) which provides that in determining whether or not a directory should be published, the Commissioner is to have regard to the need to assist members of the public to obtain personal information and to effectively exercise their rights under the Act.
- 3.11.3 The section is modelled upon section 20 of the Official Information Act which requires the production of a periodic publication setting out the functions of departments and organisations (that is, central government agencies). That publication was originally the responsibility of the State Services Commission but from 1989 was taken on by the Ministry of Justice.
- Worth of directory questioned*
- 3.11.4 This provision introduced in the Privacy of Information Bill would have imposed a mandatory function on the Commissioner. My advice to the Select Committee was that it ought to be recast as a discretionary function so that I could consider a directory amongst other priorities having a call upon my budget. My view was that the directory would have a very low call on my priorities. Realistically, I see no prospect of ever publishing a comprehensive directory of the type anticipated by section 21.
- 3.11.5 The impression I have gained from jurisdictions which require the production of a directory is that a lot of resource is consumed for very little public benefit. Frequently the production of directories is such a large task for small commissioners’ offices that it affects the orderly processing of other work. It can be a struggle to get the directory to publication in a timely fashion and published directories quickly fall out of date. “User pays” policies mean that the high price of the publication puts it beyond the reach of individuals.⁶⁷ The use of websites is a more promising option for the disclosure of information practices and policies.⁶⁸

**RECOMMENDATION 40:**

Consideration should be given to repealing section 21. Consequently section 13(1)(d) should be repealed and the content of section 21(1)(a) to (f) transferred to a rewritten section 22.

⁶⁷ The *Directory of Official Information* currently costs \$99.

⁶⁸ The USA has stressed this approach by requiring at state and federal levels public bodies to post certain information pursuant to various “Electronic Freedom of Information” laws and policies.

Directory of Official Information

- 3.11.6 A directory may be of some value in relation to the core public sector - government departments and organisations. These agencies are often large and bureaucratic, or small and obscure, and a directory may diminish barriers to individuals effectively exercising their rights under the Act. It may also be desirable for government agencies to publish their holdings of personal information to promote transparency and public accountability. On my present resources it would not be feasible for me to contemplate a public sector directory. However, others may see a value in such a directory and it might be feasible for them. Another option would be to make it a goal to include this information on websites which can be accessed from home or public libraries.
- 3.11.7 The Ministry of Justice already has the task of preparing and publishing at 2 yearly intervals, the *Directory of Official Information* under section 20 of the Official Information Act. It might not significantly increase the size of that task to include some of the categories of information listed in section 21 of the Act. Efficiencies would be possible compared with the preparation of a stand alone directory of personal information. With respect to central government I believe it is more appropriate for a Ministry to publish the directory than an independent Commissioner.⁶⁹ It may first want to review the usefulness and actual usage of the existing directory.
- 3.11.8 Two items in section 21 which might most easily be included in the *Directory of Official Information* are those set in section 21(1)(a) and (f).⁷⁰ It is not clear that section 21, or section 20 of the Official Information Act, would have to be amended to achieve the change. Perhaps the Ministry could simply add details to the directory if it judges those to be worthwhile and able to be done in a cost-effective manner. Accordingly, I provide my recommendation as a suggestion for the Ministry to consider.⁷¹
- 3.11.9 My recommendation to consider combining the task with the role of producing the *Directory of Official Information* is consistent with views expressed in the 1987 options report to the Minister of Justice.⁷²

**RECOMMENDATION 41**

Consideration should be given to the costs and benefits of having the Ministry of Justice include some of the information listed in section 21(1) in any future Directory of Official Information.

Compliance costs

- 3.11.10 If my recommendation to repeal section 21 is not adopted, I will be left with the discretionary function of publishing directories. It is not my present intention to publish any such directory. However, the power could be utilised in the future in a way that could cause compliance costs out of proportion to the benefits achieved.

⁶⁹ The *Directory of Official Information* has never, for example, been the responsibility of the Ombudsmen. In Canada, although there is both an Information Commissioner and a Privacy Commissioner, the task of collating and publishing *Info Source*, a directory that combines details required under both the Access to Information Act and the Privacy Act, falls upon the Treasury Board Secretariat.

⁷⁰ Indeed, it appears that the Information Authority considered that an obligation to list such information already existed under section 20 of the Official Information Act. See Report of the Information Authority on the subject of collection and use of personal information, May 1998, AJHR E27B, paragraph 37 and draft clause 27I. The Information Authority canvassed an alternative to having a directory which would have involved departments having a document, setting out personal information held, at each of their public offices.

⁷¹ The same exercise could be considered in respect of local authorities. They already have extensive obligations to publish information pursuant to section 19 of the Local Government Official Information and Meetings Act 1987 and it may not be problematic to add the two categories suggested. Again, I suggest this for consideration but do not have a firm view as to the merits or costs.

⁷² Tim McBride, *Data Privacy: An Options Paper*, 1987, paragraph 7.83.

“Information legislation is built on the premise that you have to know where to find information before requesting it. The Directory of Official Information is designed to fulfil this purpose under the Official Information Act; in the absence of a similar Privacy Act [directory] the privacy officer fulfils a similar role.”

- NZ LAW SOCIETY PRIVACY WORKING GROUP, SUBMISSION G22

- 3.11.11 Accordingly, I suggest that section 21(3) should direct the Commissioner to have regard not only to the need to assist members of the public but also to the compliance costs that would be imposed upon agencies in relation to the preparation of such a directory. I make this suggestion to give some reassurance that the power would be used sparingly having regard to the cost that would be imposed in complying with demands for such information. The direction would supplement the more general considerations set out in section 14.



RECOMMENDATION 42

Section 21(3) should be amended so that the Commissioner is obliged to have regard, in determining whether or not a directory of personal information should be prepared, to the compliance costs to agencies consequent upon such a determination.

3.12 SECTION 22 - Commissioner may require agency to supply information

- 3.12.1 I am empowered to require agencies to supply information that I may reasonably need for the publication of a directory of personal information or to enable me to respond to public enquiries concerning general matters connect with the holding of, and access to, the personal information by the agency concerned. I have not published a section 21 directory and therefore have not exercised the power for the purpose set out in section 22(a). However, I have used the power for the purposes provided for in section 22(b) so as to enable me to respond to public enquiries. Indeed, it is section 22(b) which holds the greatest possibilities from my perspective.
- 3.12.2 I have indicated at paragraph 3.11.4 that I am unlikely ever to publish directories under section 21. However, I do see it as an appropriate use of my office to seek out necessary information, relying upon the legal powers in section 22 where necessary, so that interested individuals can find out the sort of details which might otherwise be included in such a directory.
- 3.12.3 My enquiries team frequently question agencies to find out certain details so as to respond to enquirers. For example, an individual who wishes to obtain personal information from an agency may become exasperated through being unable to find the right person to speak to in order to obtain access to necessary records. They may call my privacy hotline. In turn, my enquiries officers through their existing contacts, or by making a specific enquiry of the agency, may find the name of the relevant privacy officer and put that person in touch with the individual. In other cases, the information sought from the agency may be more detailed but still be of the type contemplated by section 21. Such dealings are usually informal and carried out with of co-operation from the agencies concerned.
- 3.12.4 On only one occasion have I formally exercised my powers under section 22(b). On that occasion I sought from the Northern Regional Health Authority details concerning their personal information holdings about patients. On that occasion it took eight months to obtain full details. The resultant information was made available to enquirers who had been unable to get the information for themselves.
- 3.12.5 I have taken section 21(f), which refers to the steps that should be taken by an individual wishing to obtain access to personal information held by any agency, to include the identity and contact details of an agency's privacy officer. Often when a "road block" is encountered in obtaining access to information it is only by reference to a person within the agency knowledgeable in the requirements of the Act that proper explanations can be obtained as to why information is withheld or, if a mistake has been made, for the error to be rectified. If there is

doubt that the identity of the Privacy Officer is implicit in section 21(f) it may be desirable, because of the use made under section 22(b), for the matter to be made explicit.



RECOMMENDATION 43

An appropriate amendment should be made to section 21(1) or 22 so that it is plain the Privacy Commissioner has the power to obtain from an agency the identity of the agency’s privacy officer to enable the Commissioner to respond to enquiries from the public.

3.13 SECTION 23 - Privacy officers

3.13.1 Section 23 provides that each agency must ensure that there is a privacy officer to undertake certain responsibilities. It has been successful as a statutory mechanism to introduce the law to a variety of agencies in the public and private sectors and to ease compliance. A heavy handed approach is not taken and there is no specific offence of failing to appoint a privacy officer. Many businesses have seen the benefit of giving the responsibilities of a privacy officer to an appropriate employee and providing that person with the necessary authority, support and training.

3.13.2 I have observed a variety of approaches taken to appointment of the privacy officer to suit the style of particular agencies. Some have assigned a senior executive to the post who has, after developing suitable policies, delegated some of the functions. Others have devolved functions to three or four district or assistant privacy officers. Some agencies routinely involve their privacy officers in the handling of access requests whereas others retain the privacy officer as a more dispassionate internal reviewer of cases where difficulties are struck.

3.13.3 In the first months of the Privacy Act privacy officers were, in many cases, very much “on their own” (although they could, and many did, ring my privacy hotline). I am pleased to say things have since improved and now there are:

- books, and other publications, on complying with the Privacy Act;
- training opportunities through my office and other organisations;
- annual Privacy Issues Forums with, in recent years, an associated privacy officers meeting;
- some informal groupings of privacy officers in particular sectors - perhaps the most active has been those from public hospitals.

3.13.4 I continue to believe that there is significant value in the position of privacy officer and that the provision is still needed. My views in this regard were reinforced by consultation in the course of this review. In the context of complaints, I have observed that agencies with capable and experienced privacy officers have far less difficulty in resolving matters satisfactorily. A steep learning curve is required for an agency without a privacy officer if they start studying the Act when the first complaint is received.

Appointment of outside privacy officers

3.13.5 Although I take the view that section 23 is adequate, and has worked well, I propose one small change. Presently the section states that it is the responsibility of each agency to ensure that there are “within that agency” one or more individuals who have the responsibilities set out in the section. I propose that the words “within that agency” be omitted. In most cases the appropriate person to have the responsibilities of privacy officer will be an individual within the particular agency. However, there may be instances where an individual outside the agency would satisfactorily fulfil the role. Amendment to the section may provide the flexibility to enable such people to take on the role.

3.13.6 I offer as an example a franchised video library. It might be a small business

“Tranz Rail submits that the privacy officer provision has generally worked well. However, privacy officers probably need more education.”

- TRANZ RAIL, SUBMISSION G18

with, say, a manager and six or seven staff and yet be the repository of large holdings of personal information. However, across a city there might be seven or eight franchised businesses run on identical lines. It might be possible to have an individual who is not within the agency - since the franchised businesses are separate agencies - do an excellent job as privacy officer through familiarity with the information aspects of the business. Such as officer may, at less cost than doing so in separate agencies, obtain experience with compliance issues and complaints handling. He or she may also have a degree of independence from the day to day decisions that gave rise to a complaint, thereby offering a degree of detachment which can facilitate resolution of a customer or employee complaint.

- 3.13.7 It would be possible for some businesses to offer their services as a privacy officer. While lawyers or accountants might feel able to offer such a service to corporate clients the model I had in mind is something akin to the companies that provide “body corporate” services to blocks of apartments. It may also be that an experienced privacy officer might on retirement wish to spend a few hours a week, or days a month, offering contract services as a privacy officer to former employer or to agencies in the sector that he or she formerly worked in. I know of examples where departments and corporate bodies, have brought onto their staff, on a part-time basis, a trusted former employee to act as the privacy officer. I have seen this work well with experience and detachment combined to achieve excellent resolution of complaints and encouragement of compliance.
- 3.13.8 I should add that I see the opportunity for outside privacy officers as being quite limited. In most cases the ideal candidate for privacy officer will already be on staff and that is where the responsibilities should lie. However, in certain limited circumstances I can see a case for a niche “privacy officer firm” or an individual taking on the task for a number of separate agencies. I believe that the Act should allow the flexibility for these developments to occur.



RECOMMENDATION 44

Section 23 should be amended to delete the words “within that agency”.

Privacy officer support

- 3.13.9 I have two further observations in respect of privacy officers notwithstanding that the Act need not be amended to address either.
- 3.13.10 First, I encourage management of agencies to offer support and training for their privacy officers. A well informed, and proactive, privacy officer is the best friend that an agency can have to avoid problems under the Privacy Act. There are publications now available and agencies should obtain these so that the officers have the resources they need. Training should be allowed for.
- 3.13.11 Second, there is greater scope for privacy officers themselves to pool their experience, establish networks, and generally benefit each other. I know that the CHEs privacy officer group has met regularly over the years and that this has benefited the participants greatly. Smaller and less frequent meetings of privacy officers in the insurance and banking areas have also yielded benefits. I have encouraged privacy officers to organise groupings of their own but have declined to attempt any formal organisation myself - other than to offer an annual get-together at the Privacy Issues Forum.
- 3.13.12 There may be value in privacy officers examining the merits of formalised networking and organisation if the full benefits of co-operation are to be realised. In the United States there has for many years been an American Society of Access Professionals (ASAP) which offers training and education to US Federal Government employees on both the Privacy Act and the Freedom of Informa-

“Section 23 has worked well - appointment of a Privacy Officer allows focus for the setting up of procedures and education.”

- FRANKLIN DISTRICT
COUNCIL, SUBMISSION G3

tion Act. Since at least 1987 there has been a Canadian counterpart organisation for access and privacy coordinators. Something similar exists in the UK. I am not in a position to know whether that degree of organisation will suit New Zealand privacy officers but I do know that there is much to be gained through networking and that if such an organisation were to exist it would be possible to further develop the support and training of those people given the important responsibilities outlined in section 23.

3.14 SECTION 24 - Annual report

- 3.14.1 Section 24 requires me to make an annual report on the operation of the Act to the Minister of Justice, who in turn is to lay a copy of the report before Parliament. I submitted two annual reports under the Privacy Commissioner Act 1991 (the first for a part year) and four further reports under the 1993 Act.
- 3.14.2 I have endeavoured to provide a very full annual report on my activities since this is a reference point for a wide variety of people interested in the Act. Also, for certain aspects of my work, this is the only, or most convenient, place to describe some aspects of the work of the office.
- 3.14.3 However, my practice has been to regularly release and actively disseminate material from my office as an important facet of my education and publicity functions. For instance, I publish case notes of the opinions that I have reached on a range of complaints. These case notes are released individually or in batches during the year - I do not republish them in the annual report. I believe that an active dissemination policy is of most value to the public and is consistent with my commitment to freedom of information.
- 3.14.4 It would be desirable to enable my annual report on information matching programmes to be submitted separately from my general annual report. The practical difficulty I have found is that I have been delayed in submitting my annual report because of the need to await departmental reports on the last matching runs held during any financial year. Consequently, the report on my own activities tends to get held up. Conversely the report on information matching often has to be finalised in haste when the last departmental reports are to hand. The two types of reports differ in nature. The section 24 report is an account of the activities of my own office. The section 105 report is primarily a commentary upon the activities of other agencies. I propose a change to address this problem in recommendation 131.

3.15 SECTION 25 - Further provisions relating to Commissioner

- 3.15.1 The provisions in the First Schedule are primarily of a machinery nature and deal with such matters as the appointment of expert staff, salaries and allowances, superannuation, the provision of goods and services, and financial arrangements.
- 3.15.2 The use of a schedule for such matters is valuable in uncluttering the Act itself. By removing such matters to a schedule ordinary users of the Act, who have no need to know these machinery provisions, are able to move straight to provisions of greater relevance and importance. On reflection, I take the view that there are further provisions in Part III of the Act which could have suitably appeared in the Schedule.⁷³ However, there is little point now in transferring such provisions.
- 3.15.3 I have considered the provisions in the First Schedule and have identified two changes which would be desirable. One turns upon a point of principle and the other simply reflects changed circumstances.

“The provision relating to privacy officers is a useful one particularly so far as the public sector is concerned. When newspapers are requesting information and that request is refused because of the Privacy Act it is occasionally beneficial to be able to talk to the relevant privacy officer to discuss the matter further. We find it ironic that there is no corresponding duty on public sector agencies to appoint officers with similar responsibilities under the Official Information Act.”

- COMMONWEALTH PRESS UNION,
SUBMISSION G17

⁷³ For example, provisions concerning a Deputy Commissioner and continuation in office after expiry of term.

First Schedule: Clause 2 - Staff

3.15.4 Clause 2(3) of the First Schedule provides that:

“The number of persons that may be appointed under this clause, whether generally or in respect of any specified duties, or class of duties shall from time to time be determined by the responsible Minister.”

3.15.5 It seems that this provision does not sit well with the independence of my position nor the modern approach to accountability epitomised by the Public Finance Act 1989. Accordingly, I consider that it should be deleted.

3.15.6 Given the existence of the Public Finance Act, and the Memorandum of Understanding that exists between the Minister of Justice and the Privacy Commissioner, I suggest it is unnecessary to replace the provision with anything else. However, it would be possible to devise a replacement provision which did not encroach upon the Commissioner’s independence. For example, I would have no concern with a clause which provided:

The number of persons appointed under this clause shall from time to time be advised to the responsible Minister.

**RECOMMENDATION 45**

Clause 2(3) of the First Schedule should be repealed so that the Minister does not have the function of determining how many staff the Commissioner engages whether generally or in respect of any specified duties.

First Schedule: Clause 6 - Services for Commissioner

3.15.7 Clause 6(2) of the First Schedule provides that the Commissioner and the Human Rights Commission may enter into arrangements for the provision by the Commission of office accommodation and other services. At the time that the Privacy of Information Bill was being drafted this was a possibility although it has not proved to suit the needs of my office under the Privacy Commissioner Act 1991 or the 1993 Act. At one stage, I examined the possibility of shared accommodation in the event that I were to establish a Christchurch office. I considered this in the context of an invitation extended to me by the Ombudsmen to consider the possibility of sharing new premises. There were some attractive features of sharing accommodation with the Ombudsmen in Christchurch but the timing was not propitious for me to establish a South Island presence and subsequently funding difficulties would make this an impossible proposition.

3.15.8 However, exploring the Ombudsmen’s invitation emphasised to me that clause 6(2) was limiting in terms of the arrangements that might be reached with regards to the provision of services. Matters have now moved on such that I suggest that subclause (2) be repealed or amended. If it were repealed I would not see this, in any sense, as restricting my ability, or that of the Human Rights Commission, to enter into an arrangement for the sharing of services if that were appropriate. However, if the provision were to remain it could be changed to reflect the reality which is that arrangements might also be reached with other similarly placed entities such as the Ombudsmen.

**RECOMMENDATION 46**

Clause 6(2) of the First Schedule should be repealed as being unnecessary.

3.16 SECTION 26 - Review of operation of Act

3.16.1 Section 26 requires the Commissioner to review the operation of the Act as soon as practicable after it has been in force for three years and thereafter every

five years. The Commissioner's findings are to be reported to the Minister of Justice who is to lay a copy of the report before Parliament. This is, of course, the provision pursuant to which this review is being undertaken.

3.16.2 It is quite usual for modern privacy or data protection laws to include a review clause of some sort. For example, the privacy laws in British Columbia and Nova Scotia, and the private sector privacy law in Quebec were all passed at about the same time as the Act and each contained a provision for review. The Nova Scotia and Quebec reviews were completed in 1996 and 1997/98 respectively.⁷⁴ The review in British Columbia is ongoing.⁷⁵

3.16.3 Although the section does not require me to undertake public consultation, or otherwise direct how the review to be carried out, I have undertaken very full public consultation. After I launched the public phase of the review, debate was sparked in the print media as to the appropriateness of placing the section 26 review role with the Privacy Commissioner. The debate was kicked off by an article by an MP which stated, amongst other things:

“The Act has an unusual and unfortunate provision. It requires the Privacy Commissioner to review his own Act and to report to the Minister of Justice whether any amendments are necessary or desirable. This is not the way to protect the interests of the public. The Minister should amend the legislation to provide for an autonomous body, independent to the Privacy Commissioner, to review the Act.”⁷⁶

3.16.4 This drew a ready response from some newspaper editorial writers who have campaigned against privacy rights for individuals. The *Evening Post* stated:

“The public might have more confidence in the review process if it is carried out by someone seen as totally impartial. As it is, Mr Slane is widely perceived - we believe correctly - to have a strong ideological commitment to the privacy principles outlined in the Act.”⁷⁷

3.16.5 The newspapers' position may be judged from the introduction to a booklet published by the Newspaper Publishers Association and Commonwealth Press Union in 1997:

“The newspaper industry's view of the Privacy Act has been consistent since before its enactment. We saw no reason for the Act to exist and we still do not.”⁷⁸

3.16.6 It is understandable that those who are openly hostile to the Privacy Act may fear that the Privacy Commissioner will not share their views. However, I doubt

“There will be a review by Commissioner in 3 years' time and that process will continue at 5-yearly intervals. That is to be expected because of the changes that are being made day by day. Everyone who looks at the *Dominion* on Monday mornings and sees the changes in computer technology could see that the House cannot predict what is likely to happen over the next few years, and the appropriate procedure is to ensure that there are reviews at regular intervals”.

- ROB MUNRO MP ON THE SECOND READING OF THE PRIVACY OF INFORMATION BILL, APRIL 1993

⁷⁴ See Department of Justice, *Advisory Committee Freedom of Information and Protection of Privacy Act Report*, Nova Scotia, March 1996, Commission d'accès à l'information, *Privacy and Openness in the Administration at the End of the 20th Century* (abridged version of the Report on the Implementation of the Act Respecting Access to Documents held by Public Bodies and the Protection of Personal Information and the Act Respecting the Protection of Personal Information in the Private Sector), Quebec, June 1997 and Quebec National Assembly Committee on Culture, *Study on the Five Year Report of the Commission d'accès à l'information: Final Report*, April 1998.

⁷⁵ Several hearings of the Special Committee to review the Freedom of Information and Protection of Privacy Act have been held and transcripts of proceedings are available on the website of the British Columbia legislature. That can be accessed through the homepage of the Information and Privacy Commissioner of British Columbia: <http://www.oipcbc.org>

⁷⁶ Patricia Schnauer, “Too Much Autonomy for Commissioner”, *National Business Review*, 19 September 1997.

⁷⁷ “Right Man for Privacy Review?”, Editorial, *The Evening Post*, 21 October 1997.

⁷⁸ NPA/CPU, *Privacy: A Need for Balance*, 1997, page 4.

that a commitment to the privacy principles should disqualify me from carrying out a satisfactory review. It should also be borne in mind that in carrying out this function I am guided by section 14, which requires me to have due regard to, amongst other things, the interests that compete with privacy and the right of business and government to achieve their objectives in an efficient way. There seemed to be an assumption that it was within my statutory review to advise Parliament to repeal the Act. It was not my function to do so and any other reviewer of the Act would find, as I have, that there is no groundswell of opinion for such a move.

- 3.16.7 I think it should be plain to anyone who took the trouble to read the discussion papers that they encouraged, and did not limit, debate about the Act. Furthermore, I have undertaken to supply copies of *all* the submissions received to the Minister of Justice so that he will have the views of others as well as any recommendations.⁷⁹
- 3.16.8 This report as to whether any amendments are “necessary or desirable” is not the end of the process. The Minister will consider my recommendations and I would be surprised if every single one is adopted. Rather, he will first take advice from the Secretary for Justice. If amending legislation is contemplated consultation would be undertaken by the Ministry with other government departments. Once Cabinet has settled its policy, an amending bill would be introduced and referred to a select committee. Public consultation will again be had and the committee will form its views on which of the Government’s proposals for amendment, and others suggested by submissions, are desirable. Parliament itself makes the final decision. My review is hardly likely to be the last word on the subject.
- 3.16.9 The MP’s article criticised section 26 as an unusual provision. It is true that only a minority of statutes have a review provision. However quite a number do⁸⁰ and section 26 is by no means unique. Most reviews required by statute are carried out by entities established by the particular statute. The approach appears to be that the public body most intimately involved with the carrying out of functions under the statute ought to examine the issues and provide recommendations. If there is no organisation created by the statute suitable to carry out the review, the function is placed with the department or ministry. I have identified one statute which provides for a joint review by an entity established by the Act and the administering department.⁸¹
- 3.16.10 If it were to be desired to have someone other than the Commissioner carry out future reviews, there would need to be someone to do the task. One possibility would be to keep section 26 much as it is now but to place the function with the Ministry of Justice. That would have several disadvantages. In particular, it would leave no separate or knowledgeable source of advice to the Minister on the recommendations for reform - unless, of course, one imagines the Privacy Commissioner and Ministry of Justice switching present roles.
- 3.16.11 The other models that are sometimes used for reviews of this type overseas are

“The Privacy Commissioner is required to be an advocate for privacy of the individual. That’s fine except that the Office of the Privacy Commissioner also has quasi-judicial functions so it’s a bit like a rugby game where the other team’s coach acts as referee. Those who deal with the Privacy Commissioner do not doubt his sincerity or the fact that he attempts to be even-handed, but lets face it - the role of the Office of the Privacy Commissioner is to be on the side of individual privacy. A better solution would be to remove this role to a separate body which does not have any advocacy role.”

- PETER HATTAWAY,
SUBMISSION S16

⁷⁹ All non-confidential submissions were given to the Ministry of Justice in February 1998. The submissions have also been available at my office for anyone to inspect and to purchase copies.

⁸⁰ Examples of statutes having similar review provisions: Contraception, Sterilisation and Abortion Act 1977, section 14; Electricity Act 1992, section 158; Foundation for Research, Science and Technology Act 1990, section 12; Health and Disability Commissioner Act 1994, section 18; Legal Services Act 1991, section 112; Wheat Industry Research Levies Act 1989, section 30. Examples of provisions which concern the review of only one Part of an Act include: Evidence (Witness Anonymity) Amendment Act 1997, section 4; and Medical Practitioners Act 1995, section 75. These latter tend to be “one-off” rather than continuing reviews and are carried out by the administering departments.

⁸¹ See Foundation for Research, Science and Technology Act, section 12.

the creation of an *ad hoc* review body or the conferring of the function on a Parliamentary committee. It is easy to understand why the establishment of machinery and funding for a series of 3 and 5 yearly *ad hoc* review committees is not favoured.⁸² However, it is always possible for the Minister to ask the Law Commission to review an aspect of the Act as he recently did in relation to the Official Information Act. This need not await, or replace, the section 26 review.

- 3.16.12 Canadian jurisdictions typically confer the review role upon a Parliamentary committee. However, conferring such functions by statute on Parliamentary committees is not a general practice in New Zealand. Furthermore, since the mid-1980s virtually all bills are sent to a select committee which takes public submissions. Our process therefore already involves a Parliamentary committee. Adoption of the Canadian process could conceivably limit the diversity of input into the review rather than expand it and still involve my office conducting a detailed review to place before the committee.
- 3.16.13 In my view, regular review of the Act's operation is desirable and it is an appropriate function to confer on the Commissioner as demonstrated by overseas and local practice. The five yearly frequency of reviews is appropriate and I would not wish to see it lengthened or shortened. I considered that the first review should be completely open and wide-ranging and set out the reasoning for changes or for rejecting any change. Subsequent reviews may be more specifically focused.

⁸² Sometimes legislative machinery is provided for the convening of an *ad hoc* review committee for one-off reviews. See, for example, Insurance Companies (Ratings and Inspections) Act 1994, section 24.

Bouquets and Brickbats

THE REVIEW PROCESS

“The approach taken to this consultation and the simple layout of the discussion papers has been much appreciated.”

- FRANKLIN DISTRICT COUNCIL, SUBMISSION G3

“The review is very comprehensive and a number of useful points have been raised. However it may have been more useful if the review was phased in over some months with organisations being given more time to evaluate the papers.”

- NZ DEFENCE FORCE, SUBMISSION S24

“We are aware that there has been some criticism of the credibility of the section 26 review, probably because the responsibility for the review lies with an office established by the Act. The content of some of the discussion papers suggests that considerable effort has been expended to ensure the opportunity for all view points to be expressed.”

- NZ BANKERS' ASSOCIATION, SUBMISSION S25

“We do appreciate that the papers were sent out well in advance of the October and November closure dates, and congratulate the Commissioner's Office on recognising that substantial notice is required, if community organisations are to have time to consult their constituents about the issues raised.”

- NZ FEDERATION OF FAMILY BUDGETING SERVICES, SUBMISSION S29

“We found that the order in which the discussion papers were released has complicated consideration of the issues and limited the ability of staff to have helpful input.”

- FAMILY PLANNING ASSOCIATION, SUBMISSION S45

Part IV

IV

Good Reasons for Refusing Access to Personal Information

145

“A civil servant’s knowledge that an individual file is in fact accessible has a practical influence on promoting the accuracy and relevance of data.”

- David H Flaherty, *Protecting Privacy in Surveillance Societies*, 1989

“Although there has been a wide acceptance of the proposal that there should be a general right of access, there has been a great deal of debate on the question to what extent that right should be circumscribed to ensure that the privacy interest protected by a right of access is properly balanced against other legitimate interests. Those other interests include the interests of society at large. An unlimited right of access would mean, for example, that police intelligence and other records, used to prevent and detect breaches of the law, would be open to inspection by the very people whose activities they were designed, in the public interest, to frustrate. Again, there are the interests of record keepers which need to be protected. These interests might well be jeopardised unreasonably if access were to be given to all personal information which the record keepers hold.”

- Australian Law Reform Commission, *Privacy*, 1983

“An individual’s right of access tends to make the legislation self policing. It forces agencies to consider how they handle the personal information of customers and whether or not that information is accurate. This is of benefit not only to the individuals concerned but also to agencies.”

- NZ Law Society Privacy Working Group, submission L23

4.1 INTRODUCTION

4.1.1 The right of access by the individual concerned to personal information is one of the most significant entitlements in any privacy law. I was therefore pleased to receive 50 submissions on the discussion paper on access and correction - more than were made on any of the other 11 discussion papers. This chapter covers the Act’s withholding grounds and it should be read together with the material on principle 6 at paragraph 2.8, and the following chapter on procedural provisions.

4.1.2 Notwithstanding the importance of the right of access it cannot be absolute. There are competing private and public interests which need to be balanced against the individual’s right of access. However, if the right of access is to be meaningful the reasons for withholding must be very carefully circumscribed and subject to independent review. Part IV sets out “good reasons for refusing

access to personal information”. There is a finite list of such grounds and agencies are not generally permitted to withhold information for any other reason.¹ Clause 4 of the OECD Guidelines indicate that exceptions to the right of access, and other principles, should be “as few as possible.”

- 4.1.3 New Zealanders have had access rights to personal information held about them in the public sector since 1982 (central government) and 1987 (local government, education and health agencies). When the provisions governing access to personal information by the individual concerned were transferred from the Official Information Act to the Privacy Act the rights were extended to include both public and private sector agencies. However, the grounds for withholding information essentially remained the same.
- 4.1.4 Accordingly, in reviewing the grounds for withholding I have taken account of the fact that many of these provisions have existed in law since 1982. This has meant that a certain jurisprudence has grown up in interpreting the sections which should not be lightly discarded. Opinions of the Ombudsmen have been rendered on the provisions between 1983 and 1993. As the personal rights of access to information held in the public sector are “legal rights” it has been possible for individuals to also seek court judgments which offer further guidance. Since 1993 I have given my own opinions on the provisions and there have been a number of Complaints Review Tribunal decisions.²
- 4.1.5 I have borne in mind in considering possible change that there are advantages in remaining with the existing withholding grounds in some instances so as to retain the benefit of the jurisprudence developed to date. In respect of at least some of the provisions, corresponding provisions continue to exist in the Official Information Act.³

Legislative history

- 4.1.6 The Official Information Act 1982 was the outcome of recommendations of the Committee on Official Information (the “Danks Committee”) set up to study freedom of information and to review the Official Secrets Act 1951. The 1982 Act gave everyone the right to access information held by certain public sector bodies covered by the legislation and gave the individuals concerned special access rights to their own information under Part IV. The bodies covered were subsequently extended and now include, among others, government departments, state-owned enterprises, educational institutions, hospitals and others, such as my own office. The Local Government Official Information and Meetings Act 1987 applied a similar regime to local authorities.⁴ With the overall right of access was a special right for individuals to have access to personal information about themselves held by any of those bodies. There were fewer grounds for withholding that person’s information and no charge might be made for such access. For convenience a table of corresponding provisions in the official information statutes is set out in Appendix H.
- 4.1.7 In 1993 that individual right of access to personal information under Part IV was transferred to the Privacy Act, and at the same time it was applied to the private sector as well as the public sector. By and large, the grounds under the Privacy Act upon which any agency can decline to disclose to the requesting individual what it holds are the same as those previously applicable under the Official Information Act. Some of the withholding grounds may be relied upon by public sector agencies only.

¹ Privacy Act, section 30.

² My office published a compilation of Tribunal decisions in September 1997.

³ The main corresponding provisions are those relating to procedure and access to personal information by corporate bodies (see Parts II and IV of the Official Information Act).

⁴ The bodies covered by the two official information statutes corresponds generally to “public sector agency” defined in section 2 of the Act.

4.1.8 It is opportune to question whether the withholding grounds remain appropriate in their present form. As the grounds were originally drafted only to apply to the public sector it is also appropriate to consider whether or not they have proved suitable for private sector agencies and whether any new grounds should be added.

Law Commission review

4.1.9 The Law Commission received a reference from the Minister of Justice in 1992 to undertake a “fine tuning” review of aspects of the Official Information Act. That review was delayed. The Law Commission published its report in October 1997.⁵

4.1.10 The Law Commission analysed a number of provisions in the Official Information Act which are similar or identical to provisions in the Privacy Act. Accordingly, I have taken care to consider the Law Commission’s analysis and recommendations. In some cases, I have adopted the Law Commission’s recommendations for similar amendments to the Privacy Act. It is not essential for provisions in the two Acts to be identical as the statutes have different coverage and serve somewhat different purposes. However, it may be beneficial where practicable to maintain a general consistency between the statutes in certain areas. In some cases, my recommendation for change to the Act is accompanied by a suggestion that similar change be considered for the official information legislation.

4.1.11 The interaction between the Act and the official information legislation is such that I am fortunate that the Law Commission completed its review at the time that it did. However, that review was of limited usefulness from my perspective as the terms of reference were established in 1992 and did not touch upon some of the new issues apparent by 1997/98. This might point to the desirability, at some future point, of programming a concurrent review of aspects of the procedural provisions and withholding grounds in the Privacy Act and Official Information Act by the Ministry of Justice. For this reason I have offered some suggestions for further consideration even where I do not recommend immediate change to the Privacy Act.

Grouping of withholding grounds

4.1.12 It will not be apparent why the reasons for refusing a request are split into three groups: sections 27, 28 and 29. The grounds for withholding in section 27 of the Official Information Act were carried into the Act. That section in turn refers to other sections in the Official Information Act. The rather perplexing grouping of withholding grounds in sections in the Privacy Act 1993 is attributable to the way in which the grounds for withholding in respect of official information and personal information are broken down in sections 6, 7 and 9 of the Official Information Act.

4.1.13 The key aspect of the structure of the Official Information Act appears to be that the grounds for withholding in section 6 are identified as “conclusive” reasons for withholding information - a distinction not used in the Privacy Act. The other grounds do not have this “conclusive” status and are set out in section 9 with some special reasons separated into section 7. However, if one compares the breakdown in sections 27 to 29 of the Privacy Act the reason for the structure is not immediately clear. The confusing arrangement makes the Act more complex than would otherwise be the case.

4.1.14 I have therefore concluded that it would be desirable to reorganise sections 27 to 29 to better meet the needs of users of the Act. The wording of the withholding grounds should remain the same unless there is specific reason for change. I envisage three ways in which this reorganisation could be achieved.

⁵ Law Commission, *Review of the Official Information Act 1982*, 1997.

- 4.1.15 The first would place all the withholding grounds in a single section. This would have the merit of discontinuing the perplexing practice of splitting the withholding grounds into three sections. It would also mean that users of the Act would need look at only one section to locate all the withholding grounds. A significant disadvantage would be that the section would be very long. Our legislation does not follow the practice adopted in some jurisdictions of having marginal notes relating to individual subsections and therefore this option would not be particularly helpful for users to quickly locate the exact provision of relevance.
- 4.1.16 The second option would place each of the grounds for withholding in a separate section with its own marginal note. Users would be able to quickly identify if there is a provision of relevance. One minor disadvantage is that the rather unattractive alpha-numeric numbering system of sections will have to be followed (that is, section 27, 27A, 27B, 27C etc).
- 4.1.17 The third option would remove all the withholding grounds to a new schedule and allow each to have their own separate clause and heading.⁶ Parliamentary Counsel may have a view as to whether it is appropriate for this material to be so relocated.
- 4.1.18 Whichever option is adopted it would probably make sense for the reasons for refusing requests to be reordered for convenience of users. The early clauses should ideally set out the most important grounds for withholding or the ones likely to arise most frequently in practice. On this basis, the present ordering is the wrong way around. The section 27(1)(a) and (b) reasons are hardly ever relevant to requests whereas those in (c) and (d) are of considerable importance in the practical operation of the Act. Similarly, sections 27(2) and 28 are less frequently relied upon than the provisions in section 29.
- 4.1.19 Before making this recommendation I considered whether change in organisation or layout of the provisions might unduly confuse users of the Act. In my view, it will not. People who currently work with the Act, such as privacy officers and those involved in granting or refusing access, will quickly identify the new provisions because:
- they will be easy to find as each provision will have its own heading;
 - the substantive reasons for refusing requests will not have changed and familiar wording will continue to be used.
- Any modest inconvenience for existing users of the Act will be more than offset by the improved usability of the provisions in the new format.
- 4.1.20 Some consequential amendments will need to be made. Section 32 which allows an agency to neither confirm nor deny whether certain information exists will need to be amended to list the provisions to which it applies. If the provisions are placed in a schedule consideration may need to be given to whether that schedule should be expressly referred to in principle 6(3).



RECOMMENDATION 47

The existing reasons for refusal of requests set out in sections 27, 28 and 29 should be reorganised into an ungrouped list of reasons to make it easier for users of the Act to locate relevant provisions.

SECTION BY SECTION DISCUSSION

4.2 SECTION 27 - Security, defence, international relations etc.

4.2.1 Section 27 provides for the withholding of information which, if disclosed pur-

⁶ Schedules are arranged according to the order in which they are introduced in the Act. Therefore, this would presumably appear between the existing First and Second Schedules.

suant to principle 6, would be likely to prejudice certain security, defence, international relations, law enforcement, and safety interests. The section deals with the same types of interests dealt with in sections 6 and 7 of the Official Information Act.

Marginal note

- 4.2.2 The marginal note to this section is not as helpful as it might be. In particular, it fails to draw readers' attention to the fact that grounds relating to maintenance of the law and personal safety, which are much more frequently invoked, are also located within the sections. For this reason I have recommended elsewhere that the marginal note should be changed to make it more useful.⁷

27(1)(a): Security, defence, international relations

- 4.2.3 The first ground for refusing requests is where the disclosure of the information would be likely to prejudice the security or defence of New Zealand or the international relations of the Government of New Zealand. This is derived from section 6(1)(a) of the Official Information Act which in turn is closely modelled upon the provision recommended by the Danks Committee.⁸ Danks considered this withholding ground as being necessary in the interests of the country as a whole.

- 4.2.4 The withholding ground in section 27(1)(a) interacts, in relation to some aspects of international relations, with the grounds found in sections 27(1)(b) and 27(2). Similarly, in the Official Information Act there are at least five provisions dealing in a direct way with information relating to New Zealand's international relations.⁹ The Law Commission recently considered aspects of those provisions in its review of the Official Information Act as it had been asked by the Minister of Justice to consider "whether there should be special rules governing the treatment of some or all classes of diplomatic documents". That did not require a complete review of the withholding grounds and the Law Commission recommended no change to the existing law.¹⁰

- 4.2.5 Defence, security, and the conduct of foreign affairs, are areas of Government activity which have traditionally been relatively free from external scrutiny. The grounds for refusing requests for information of that type in both the Privacy Act and Official Information Act are relatively broad. However, there have to date been few complaints brought on review to my office. This is not entirely surprising since the sensitive holdings of information generally do not relate to personal information held about particular individuals but to various State secrets that agencies would wish to keep from prying eyes of researchers, the news media or other citizens. In this area, therefore the Ombudsmen have been called upon more frequently to review access complaints in the official information jurisdiction than I have in the personal access jurisdiction.

27(1)(b): Inter-governmental entrusting of information

- 4.2.6 Section 27(1)(b) provides for withholding if release of the requested information would be likely to prejudice the entrusting of information to the Government of New Zealand on a basis of confidence by another government or an international organisation. In recommending this provision the Danks Committee referred to a then recent report by the Chief Ombudsman on the Security Intelligence Service which had reached the conclusion that information received by New Zealand from its friends is of major importance in the political, economic, and strategic policy making fields. Danks had concluded that it

“Defence, security, and the conduct of foreign relations are areas of Government activity which have traditionally been relatively free from legislative and judicial scrutiny. The Official Information Act does little to disturb this relative freedom from scrutiny.”

- EAGLES, TAGGART, LIDDELL,
FREEDOM OF INFORMATION IN NEW
ZEALAND, 1992

⁷ See recommendation 2.

⁸ Committee on Official Information, *Towards Open Government: General Report*, 1980, page 17 and *Towards Open Government: Supplementary Report*, 1981, page 65.

⁹ Official Information Act 1982, sections 6(a), 6(b), 7, 10 and 31.

¹⁰ Law Commission, *Review of the Official Information Act 1982*, pages 91-97.

is in the national interest to continue to get as much of this information as possible and accordingly recommended that protection for disclosure should be absolute if disclosure is likely to prejudice essential interests including the continued flow of information.¹¹

- 4.2.7 The provision appears to have operated satisfactorily and I have received few complaints relating to its use to withhold information. In the light of this, and the recent recommendation of the Law Commission to make no change to similar provisions in the Official Information Act (albeit that the Law Commission's brief was very narrow), I make no recommendation for change at this time.

27(1)(c): Maintenance of the law

- 4.2.8 Section 27(1)(c) allows an agency to withhold personal information from the individual concerned if its disclosure “would be likely to prejudice the maintenance of the law, including the prevention, investigation and detection of offences, and the right to a fair trial.” Typically this ground has been used for the police to hold back from a suspect the details of an ongoing investigation.

Informant identity

- 4.2.9 I have followed the Ombudsmen, who applied the same wording under the Official Information Act, in forming the opinion that this provision allows an agency engaged in maintaining the law to hold back the identity of informants.¹² The argument goes that the identity of an informant, together with the information given, is personal information about the subject of that information who is therefore entitled to request access to it. This was the prevailing orthodoxy under the Official Information Act and now seems accepted by the Complaints Review Tribunal in respect of the Privacy Act.¹³ However, if potential informants were to learn that their identity could be disclosed upon request to the person against whom they are informing, they would be far less likely to volunteer any information at all. Some agencies depend upon the flow of informant information in order to carry out their law maintenance functions effectively. The disclosure of informant identity would prejudice the maintenance of the law by tending to cause that flow to dry up. Therefore, while each case is considered on its merits, it is usually possible to withhold informant identity details, where:

- (a) the agency is engaged in maintenance of the law activities;
- (b) its efficiency in those activities depends substantially upon the receipt of information from informers; and
- (c) there is reason to believe that informants would be less likely to provide the information if they knew that their identities would probably be revealed upon request.

- 4.2.10 I have taken this one step further in recognising that sometimes informants will not provide their information directly to the law enforcement body but to another agency which effectively acts as a conduit for such information in certain circumstances. Thus an informant told a school about certain persons allegedly selling drugs in the school grounds¹⁴ and another told an insurance company of an alleged fraud against it.¹⁵ In both of those cases the agency was able to withhold the informant's identity pursuant to section 27(1)(c) in my opinion.

Investigation and detection of offences

- 4.2.11 There are also a number of complaints concerning the withholding of information from individuals pending the completion of investigations. On a number

¹¹ Committee on Official Information, *Towards Open Government: General Report*, 1980, pages 17-18.

¹² See, for example, case notes 107, 115, 305, 549, 757, 2438 and 17375.

¹³ See *Hadfield v Police* (1996) 3 HRNZ 115, 118 and *Adams v Police* (CRT Decision No. 16/97).

¹⁴ Case note 2438.

¹⁵ Case note 17375.

“We are pleased to note that the Privacy Commissioner has held that section 27(1)(c) can be used to protect the identity of informants, acknowledging the disclosure of informant identity would prejudice the maintenance of the law by tending to cause the information to dry up. Sometimes informants will provide information not directly to the law enforcement agency, but to the agency directly affected, such as an insurance company, which can act as a conduit for such information.”

- INSURANCE COUNCIL,
SUBMISSION L9

of occasions I have agreed with an agency’s decision to withhold information while an investigation is continuing. In some of these cases I have issued a case note explaining the approach that I have taken.¹⁶ However, I have emphasised that the ground for withholding the information only applies until the investigation is completed. Once a decision has been made to prosecute the individual, or not to proceed any further with the investigation, information may no longer be withheld under section 27(1)(c).¹⁷

- 4.2.12 The withholding of personal information on the basis that disclosure would be likely to prejudice further investigation or detection of offences that might be committed by the requester was considered by the Complaints Review Tribunal in a case brought by an unsuccessful requester.¹⁸ The plaintiff in that case had a history of making threats which warranted investigation. The Tribunal found that the Police properly withheld details of an inquiry into a threat by the plaintiff in 1989 on the basis that disclosure would be likely to prejudice the investigation of any threats that might be made in a similar manner in the future. The Police were concerned that disclosure of these details could be used by the plaintiff to avoid detection. This is a relatively unusual circumstance since information is usually made available after a decision on a particular investigation has been made.

TAIC

- 4.2.13 The Transport Accident Investigation Commission suggested that this provision be modified. TAIC looks into accidents with the aim of furthering transport safety by identifying causes and contributing factors so that accidents may be avoided in future. The Commission, in some of its work may depend upon a flow of information from individuals who would not wish to have their identities revealed.
- 4.2.14 I canvassed the matter in the discussion paper and have received a number of submissions. I considered these and the merits of the TAIC position. I am not convinced that a new withholding ground, or a modification of existing grounds, is necessary to address safety issues generally or accident investigation issues in particular. If there is an issue with respect to this particular agency it would be more appropriately dealt with in its own legislation.¹⁹

Canadian law enforcement provisions

- 4.2.15 Modern provincial Canadian privacy and access laws spell out the law enforcement interests justifying, or not justifying, withholding with greater specificity than is the case with section 27(1)(c). For example, section 15(1) of the Freedom of Information and Protection of Privacy Act 1992 (British Columbia) sets out 12 law enforcement-related reasons for which information may be withheld. They are expressed in a plain fashion which does not invite the same degree of uncertainty as the general phrase “to prejudice the maintenance of the law”. For example, under the British Columbia law a public body may refuse to disclose information to the applicant if, amongst other law enforcement grounds, the disclosure could reasonably be expected to:
- harm the effectiveness of investigative techniques and procedures currently used or likely to be used, in law enforcement;
 - reveal the identity of a confidential source of law enforcement information;
 - reveal any information relating to or used in the exercise of prosecutorial discretion;
 - deprive a person of the right to a fair trial or impartial adjudication;

¹⁶ See case note 437 concerning an ACC investigation and case note 845 concerning an investigation by the Commerce Commission.

¹⁷ Except, for example, that information necessary to be withheld to protect informant identity as discussed above.

¹⁸ *Adams v New Zealand Police*, CRT Decision No 16/97.

¹⁹ The effect of a provision in such a statute is saved by section 7(2)(a).

“The Association does not believe that allowing TAIC to refuse to disclose personal information held about an individual to that individual will promote TAIC’s public safety function. NZALPA believes that to do so would inhibit co-operation by pilots and air traffic controllers and thereby reduce the full and free flow of information. What is at risk is the co-operative and contributive values which have characterised aviation safety culture.”

- NZ AIR LINE PILOTS’ ASSOCIATION,
SUBMISSION L6

- reveal a record that has been confiscated from a person by a peace officer in accordance with an enactment;
 - facilitate the escape from custody of a person who is under lawful detention.²⁰
- 4.2.16 The provision, in common with the general approach of Canadian legislation to access issues, also sets out circumstances in which public bodies may not refuse to give access to information. These have more relevance in the official information context than for an information privacy request (for example, requiring a report prepared in the course of routine inspections by an agency that is authorised to enforce compliance with an Act to be made available).
- 4.2.17 It is reasonably likely that a similar result will be arrived at in the application of both the New Zealand and Canadian provisions - although there may be particular, and important, differences in detail. However, the key difference is that the Canadian provision is easily understandable on its face whereas the full meaning of the phrase used in the New Zealand Act is only completely apparent when the case law, including opinions of the Ombudsmen and Privacy Commissioner, is also known.
- 4.2.18 It would be desirable at some stage for the section 27(1)(c)²¹ provision to be rewritten in such a way that it may be clearly understood by all those involved including:
- staff in law enforcement agencies;
 - requesters;
 - bodies exercising review functions.
- 4.2.19 If there is to be change it would be necessary that this be done in conjunction with consideration of similar provisions in the Official Information Act and the Local Government Official Information and Meetings Act. There is no immediate urgency as most “maintenance of the law” agencies have a good understanding of the withholding ground.



RECOMMENDATION 48

Consideration should be given to the merits of redrafting the “maintenance of the law” withholding grounds to make more plain the constituent law enforcement interests protected.

- 27(1)(d): Endangering the safety of an individual*
- 4.2.20 Section 27(1)(d) allows an agency to withhold material from an information privacy request if its disclosure “would be likely to endanger the safety of any individual.” The Complaints Review Tribunal has formed the opinion that this provision refers to physical safety, and would not allow withholding where there is a likelihood of harassment falling short of physical attack.²²
- 4.2.21 The Official Information Act allows “official information” (but not personal information about the requester) to be withheld if that is necessary for the “protection of Ministers, members of organisations, officers, and employees from improper pressure or harassment”. That ground is provided for in the context of “maintaining the effective conduct of public affairs” rather than personal safety.²³ Accordingly, there is some precedent in our information laws for considering harassment as a reason for withholding information from a requester in some circumstances.

²⁰ Section 15(1)(c), (d), (g), (h), (i) and (j).

²¹ Any rewriting of section 27(1)(c) might also incorporate 29(1)(e) concerning the safe custody of inmates.

²² *O v N (No 2)* (1996) 3 HRNZ 636. See also *M v Ministry of Health* (1997) 4 HRNZ 79 and *M v Police* (1997) 4 HRNZ 91.

²³ See Official Information Act 1982, section 9(2)(g)(ii).

- 4.2.22 I have raised on previous occasions the need to provide adequate legal protection to individuals from the threat of harassment. For example, I supported the enactment of the Harassment Act 1997²⁴ and advocated enabling electors to go on the confidential electoral roll when they had obtained restraining orders under that Act.²⁵ I have also suggested that there should be consideration of the desirability of enabling information to be withheld on an Official Information Act request where there is a likelihood of harassment of an individual as a result of the release of information.²⁶
- 4.2.23 The risk of harassment is probably more likely to arise upon an Official Information Act request or a public register request²⁷ than on an information privacy request. This is because the main circumstance in which harassment might be anticipated as the result of individuals obtaining personal information about themselves is where the identity of informants is revealed. However, identity of informants is commonly withheld under the maintenance of the law provision. However, in the Official Information Act context third party requests for a whole range of information might potentially be used for the purpose of harassment.
- 4.2.24 The Law Commission’s review of the Official Information Act was simply “fine tuning” and they were constrained by terms of reference they had been given. Accordingly, their report did not draw out any issues in relation to harassment. I consider it would be desirable for the matter to be considered and, if any change were to be warranted, for there to be similar provision in both the Privacy Act and the official information legislation.



RECOMMENDATION 49

Consideration should be given to the desirability of enabling the withholding of information where there is a significant likelihood of harassment of an individual as a result of the disclosure of information.

4.3 SECTION 28 - Trade secrets

- 4.3.1 Section 28 provides for the withholding of information in order to protect trade secrets or to avoid prejudice to certain other commercial interests. It is subject to a public interest override in that information may not be withheld if the withholding is outweighed by other considerations which render it desirable, in the public interest, to make the information available. This provision reflects section 9(2)(b) of the Official Information Act 1982 and rarely features in complaints to the Privacy Commissioner. Criticisms of the provision would probably include the following:
- section 28(1)(a) concerning “trade secrets” appears to have almost no application to information privacy requests by individuals;
 - section 28(1)(b) concerning likely “prejudice to a commercial position” is too narrowly drawn to enable withholding in all appropriate circumstances.
- 4.3.2 The marginal note is not as helpful as it might be. I have recommended elsewhere that it be changed to “trade secrets and prejudice to commercial position”.²⁸

²⁴ See Report of the Privacy Commissioner to the Minister of Justice on the Harassment and Criminal Associations Bill, January 1997 and discussion in this report at paragraphs 7.15.3 - 7.15.9.

²⁵ See Report of the Privacy Commissioner to the Minister of Justice on the Electoral Act 1993, April 1997.

²⁶ See Submission by the Privacy Commissioner to the Law Commission in relation to a “fine tuning” review of the Official Information Act 1982 on a reference from the Minister of Justice, April 1997.

²⁷ Submission S59 suggested that protesters at Wellington’s Parkview Clinic had engaged in harassment, some of which was facilitated through noting motor vehicle licence plate numbers and tracing personal details through the public register.

²⁸ See recommendation 2.

28(1)(a): Trade secrets

4.3.3 The term “trade secrets” is not defined in the Act. It is rarely cited in Privacy Act or Official Information Act cases. The Ombudsmen have commented:

“A general approach to the circumstances in which [the equivalent provision in the Official Information statutes] might apply has not been developed. It has been raised in very few cases, and where it has been raised, there have been difficulties in defining the term ‘a trade secret’.”²⁹

4.3.4 It appears from commentaries on the Official Information Act that the provision has been derived from American law.³⁰ In the USA there has apparently been debate and litigation concerning the breadth of what constitutes a “trade secret” with further divergence in other common law countries.³¹

4.3.5 That the term may not have a settled meaning is potentially problematic given that there is no statutory definition. It would be possible to await a suitable case to go to the Tribunal to provide a precedent and guidance. The wait may be protracted as it is difficult to envisage circumstances in which such a trade secret might be categorised as “personal information” about a requester.

4.3.6 It is worth questioning whether section 28(1)(a) is necessary. The Australian Law Reform Commission speculated in 1983 that “It may well be that some personal information encompasses trade secrets” but offered no concrete examples.³² The Danks Committee bill had no provision for refusing a request for personal information by the individual concerned on the trade secret grounds. Perhaps the relevance of trade secret in this context concerns the position of an employee who has been closely involved with the development of the formula, process, device etc and that the resultant information about the trade secret also comprises information about the employee? However that is hypothetical and seems unlikely to arise in practice. Another hypothetical example put forward is a personnel consultant’s questionnaire for assessing personality types or aptitudes. Perhaps an access request for a candidate might involve revealing the consultant’s “trade secrets” although it is possible that Part V of the Act can cope with this by providing a summary rather than a copy of the information. Alternatively, it might be suggested that section 28(1)(a) is intended to clearly indicate that where a trade secret is recorded in a document containing personal information that it can be deleted from the information in the document pursuant to section 43(1). This is not strictly necessary since such information is severable from the document anyway as not being personal information about the requester.

4.3.7 I accept that there is a need for agencies to be able to protect trade secrets from release in response to an access request. I simply doubt whether a specific withholding ground is even necessary since it is difficult to conceive of the information as “personal information” about a requester. Where the trade secret is in the hands of an agency other than the primary possessor of the trade secret (perhaps supplied with an application to a government agency for a licence) the trade secret can be protected on a personal access request through section 28(1)(b) or on an Official Information Act request under sections 9(2)(b), 9(2)(ba) or 18(a) of that Act.

4.3.8 However, if the reason is to remain in the Act it is desirable to provide some certainty through the inclusion of a definition. If a definition is provided it should probably be placed within section 28 itself rather than in section 2 since

²⁹ Office of the Ombudsmen, *Practice Guidelines No. 3*, September 1993, paragraph 5.2.

³⁰ See *Freedom of Information in New Zealand*, 1992, page 294.

³¹ *Ibid*, pages 293-297.

³² Australian Law Reform Commission, *Privacy*, 1983, paragraph 1273.

this is the only place that it is used. Some of the recent provincial statutes in Canada have defined “trade secret” in the following manner which appears suitable for our own Act:

“**Trade secret** means information, including a formula, pattern, compilation, program, device, product, method, technique or process that:

- (a) is used, or may be used, in business or for any commercial advantage;
- (b) derives independent economic value, actual or potential, from not being generally known to the public or to other persons who can obtain economic value from its disclosure or use;
- (c) is the subject of reasonable efforts to prevent it from becoming generally known; and
- (d) the disclosure of which would result in harm or improper benefit.”³³



RECOMMENDATION 50

Section 28(1)(a) should be repealed as being unnecessary as a reason for withholding information. However, if it is retained a straightforward definition of “trade secret” should be inserted into the provision.

28(1)(b): Prejudice commercial position

4.3.9 Section 28(1)(b) allows an agency to withhold personal information if making it available “would be likely unreasonably to prejudice the commercial position of the person who supplied the information or who is the subject of the information”. The subsection does not allow the agency to withhold personal information if the disclosure would prejudice its own commercial position which may seem odd. An example of this oddity is that an employee in the throes of negotiating a redundancy settlement may be able to seek access to a company’s board minute setting out the parameters within which the company’s executives are allowed to settle such claims.

4.3.10 If the provision were to be amended, it would require care to ensure that agencies could not use a “commercial prejudice” argument to impose a blanket of secrecy over substantial areas of personal information which they hold. However, the inclusion of the qualifying “unreasonably” in subsection (1) and the public interest test set out in subsection (2) may suffice for this. It is also an area where there would desirably be consistency between the Act and official information legislation.

4.3.11 If there were to be change, the opportunity could be taken to bring together in a more coherent way some of the provisions revolving around commercial interests - the obvious candidate being the evaluative material withholding ground in section 29(1)(b). As an illustration (but not necessarily a suitable precedent), the British Columbia legislation has the following provision:

“Disclosure harmful to business interests of a third party

The head of a public body must refuse to disclose to an applicant information:

- (a) that would reveal:
 - i) trade secrets of a third party, or
 - ii) commercial, financial, labour relations, scientific or technical information of a third party,

³³ See Freedom of Information and Protection of Privacy Act 1993 (Nova Scotia), section 3; Freedom of Information and Protection of Privacy Act 1992 (British Columbia), Schedule 1; Freedom of Information and Protection of Privacy Act (Alberta), section 1.

- (b) that is supplied, implicitly or explicitly, in confidence, and
- (c) the disclosure of which could reasonably be expected to:
 - i) harm significantly the competitive position or interfere significantly with the negotiating position of the third party,
 - ii) result in similar information no longer being supplied to the public body when it is in the public interest that similar information continue to be supplied,
 - iii) result in undue financial loss or gain to any person or organisation, or
 - iv) reveal information supplied to, or the report of an arbitrator, mediator, labour relations officer or other person or body appointed to resolve or enquire into a labour relations dispute.”³⁴

4.3.12 The provision quoted does not provide for the agency to withhold its own commercial information but, like section 28(1)(b), simply provides for the protection of third party secrets.³⁵ However, unlike section 28, the British Columbia section permits the withholding of a wider range of information which would be harmful to business interests such as information supplied to, or the report of, an arbitrator.

4.3.13 The scope for withholding information for reasons of commercial sensitivity has been controversial under the Official Information Act. In respect of certain commercial issues, or involving the trading activities of the public sector, aspects of the Danks regime have been departed from and variously amended since 1982. I have seen little point in developing a precise proposal for amending section 28(1)(b) since it would anyway have to also “pass muster” in relation to an amendment to the Official Information Act. Accordingly, I simply identify for consideration some suggestions for a future joint review, namely:

- the question of whether agencies should be able to withhold information to protect their own commercial position; and
- as a particular manifestation of that, whether a withholding ground specifically providing for information to be withheld when an individual has entered into negotiations with the agency and the disclosure of the information would unreasonably reveal the bargaining position of the agency.³⁶



RECOMMENDATION 51

Consideration should be given to amending section 28(1)(b) to provide for withholding of information where the disclosure would unreasonably prejudice the commercial position of the agency itself, particularly where the information requested would reveal the agency’s bargaining position in respect of negotiations involving the individual concerned.

4.4 SECTION 29 - Other reasons for refusal of requests

4.4.1 Section 29 completes the trio of sections providing reasons for the refusal of access requests. The provision is derived from section 27 of the Official Infor-

³⁴ Freedom of Information and Protection of Privacy Act 1992 (British Columbia), section 21(1). I have omitted subsections (2) and (3) as not being relevant to the discussion here.

³⁵ However, there is another provision in the British Columbia Act allowing the public sector agency to withhold information to protect its own interests: Freedom of Information and Protection of Privacy Act 1992 (British Columbia), section 17 (Disclosure harmful to the financial or economic interests of a public body).

³⁶ Something along these lines exists in section 9(2)(j) of the Official Information Act although this has never been a withholding ground in the personal access regime.

mation Act and section 26 of the Local Government Official Information and Meetings Act. Appendix H sets out a table which quickly identifies the equivalent provisions in those other statutes.

29(1)(a): Unwarranted disclosure of the affairs of another

- 4.4.2 Paragraph (a) allows withholding of information where disclosure would involve the unwarranted disclosure of the affairs of another individual, living or dead. Accordingly, there are two limbs to establish that good reason exists to refuse disclosure under the provision:
- the disclosure of the information would disclose the affairs of another person; and
 - such disclosure would be unwarranted.
- 4.4.3 This provision is frequently relevant where information requested is “mixed information” about both the requester and another person. I have released case notes in relation to a few of the cases on which I have reached an opinion.³⁷ The Complaints Review Tribunal has also considered the ground in cases brought before it.³⁸
- 4.4.4 Consideration of this withholding ground provides a clear example of how there can be a tension between the privacy rights or expectations of two individuals, one of whom would like to have access to information and the other who may prefer control of, or restriction on, the disclosure of that information. Cases can often be resolved through means such as:
- obtaining the consent of one individual to the release of the information;
 - giving access to a summary of information rather than the full information itself.
- 4.4.5 However, in many cases techniques such as severance of information, provision of summaries or the obtaining of consents, cannot resolve the issue and agencies, and on review I or the Tribunal, must reach an opinion as to whether the case involves the “unwarranted” disclosure of the affairs of another individual. I have sought to develop a consistent approach to the recurrent examples that come before me and in doing so have been assisted by the previous approach developed by the Ombudsmen.
- 4.4.6 This is not the place to summarise the jurisprudence that has developed in relation to the statutory provisions since that can be obtained from other sources such as my case notes, the case notes and Practice Guidelines of the Ombudsmen, decisions of the Tribunal and the various commentaries on the Privacy Act and Official Information Act. It may suffice to say that access reviews involving mixed information, and the balancing of privacy interests of two or more individuals, involve some of the most difficult complaints that come before me. Nevertheless, I consider the statutory test to be satisfactory and not in need of amendment.
- 4.4.7 However, at some future point when it is possible to give the withholding grounds in both the Official Information Act and the Privacy Act a thorough, and concurrent, review it may be possible to spell out a new set of withholding grounds which make some of the recurrent issues plainer to deal with both by agencies and on review. This ought to be achievable since a series of common approaches can be found in my case notes, those of the Ombudsmen and the guidance from courts and the Tribunal. The Canadian approach could be adopted whereby the Act spells out the common circumstances in which information must be withheld or must be released. However, while such an approach may be satisfactory

³⁷ See, for example, case notes 83, 567 and 15513.

³⁸ See, for example, *O v N (No 2)* (1996) 3 HRNZ 636, *M v Ministry of Health* (1997) 4 HRNZ 79, *M v Police* (1997) 4 HRNZ 91 and *Adams v NZ Police*, 12 June 1997, CRT Decision No 16/97.

for the recurrent issues there would remain a need for a test along the lines of section 29(1)(a) to deal with the less common situations on a case by case basis.



RECOMMENDATION 52

Consideration should be given to providing statutory guidance on the withholding of information in the common cases of “mixed” information concerning the requester and other individuals.

29(1)(b): Evaluative material

4.4.8 One withholding ground which features in many enquiries and complaints to the Privacy Commissioner is that set out in section 29(1)(b) and section 29(3) which relate to “evaluative material”. The provision has come directly from the Official Information Act. It allows an agency to withhold personal information “being evaluative material” where the disclosure would:

“breach an express or implied promise ... which was made to the person who supplied the information; and which was to the effect that the information or the identity of the person who supplied it or both would be held in confidence.”

4.4.9 Subsection 29(3) goes on to define restrictively what is meant by “evaluative material” in this section. It provides that “evaluative material” means “evaluative or opinion material” compiled solely:

- “(a) for the purpose of determining the suitability, eligibility, or qualifications of the individual to whom the material relates -
 - i) for employment or for appointment to office; or
 - ii) for promotion in employment or office or for continuance in employment or office; or
 - iii) for removal from employment or office; or
 - iv) for the awarding of contracts, awards, scholarships, honours or other benefits; or
- (b) for the purpose of determining whether any contract, award, scholarship, honour, or benefit should be continued, modified, or cancelled; or
- (c) for the purpose of deciding whether to ensure any individual or property or to continue or renew the insurance of any individual or property.”

4.4.10 The evaluative material reason for withholding is probably one of the most complicated to apply and most likely to vex both requesters and agencies. The Complaints Review Tribunal has given some guidance on the statutory tests.³⁹ The recommendations that I make will probably not diminish such difficulties as the subject matter requires careful limitation in scope, and weighing of competing interests, if it is adequately to perform its task. Possibly my recommendation to split the reasons for refusing requests into separate sections will slightly simplify matters by enabling users of the Act more readily to find the provision and by bringing the definition of “evaluative material” immediately adjacent to the provision to which it applies.

4.4.11 The evaluative material provision falls into an area where traditional views on secrecy come clearly into conflict with more modern attitudes involving openness towards employees and customers. Traditionally various pieces of information were supplied secretly to employers, insurers, and others, and decisions affecting the careers and entitlements of individuals were based upon it. As the definition makes clear, “evaluative material” concerns information which will be

“Insurance companies need to be able to withhold evaluative material relating to claims due to the fact that a claimant has the ability to request their personal information while the insurance company may be investigating the claim, thereby prejudicing the outcome of the investigation. It seems to us to be anomalous that the ACC can withhold information in an ongoing claims investigation by using section 27(1)(c), and yet there has been some question as to whether or not this same ability is extended to the private sector.”

- INSURANCE COUNCIL,
SUBMISSION L9

³⁹ *Westwood v University of Auckland* (1997) 4 HRNZ 107.



used in decisions affecting the individual. This is not trivial or inconsequential information sitting on a database never to be referred to or used. It is critical information which individuals may wish to check. In the absence of access rights, decisions may be taken on unreliable information which is not open to challenge by the person most directly concerned. I am therefore reluctant to recommend any “simplification” which might have the effect of diminishing rights of access or allowing larger segments of information to be held “off limits”. Submissions show a wide diversity of views being broadly evenly split between supporting the expansion of the provision, leaving it as it is, and narrowing it.⁴⁰

- 4.4.12 Nonetheless, within appropriate bounds, I remain of the view that there is a legitimate interest needing to be protected in relation to evaluative material. My two proposals will not significantly diminish the existing restrictions.

Meaning of “supply”

- 4.4.13 The first proposal that I have is to clarify the provision so that information generated *within* an agency by a person as part of his job cannot be withheld pursuant to this provision. One key element of the existing provision is that disclosure would breach a promise which was made to the person “who supplied the information”. Lying behind the provision is a concern, also reflected elsewhere in other reasons for withholding information,⁴¹ that information, will not be supplied on future occasions if a promise of confidentiality cannot be offered and be respected.

- 4.4.14 Evaluative material by its nature is used in decisions about an individual’s future and I am concerned that, if the provision is not carefully circumscribed, the access entitlement may be meaningless in a critical situation. In the case of the employee whose line supervisor has given a report to the employer in relation to future employment, the information should not be able to withheld pursuant to this provision (although there might be some other applicable holding ground in particular circumstances). However, that situation differs from the employer who seeks a report on a prospective employee from someone with something relevant to say who is unwilling to do so except on a promise of confidentiality.⁴² Although it is desirable that such people be willing to give comments, even critical comments, openly and on the basis that they could be shared with the individual, that does not always accord with reality. There is a public interest in ensuring that such information continues to be made available and, in limited and appropriate cases, able to be withheld.

- 4.4.15 The concern about prejudice to the future supply of information does not generally exist in relation to internally generated information. For example, if an employer asks a line supervisor for a report on an employee, the supervisor is in no position to insist on a promise of confidentiality - the evaluative comments will be supplied regardless as part of the supervisor’s job. With this in mind I have interpreted the reference to the *supply* of the information in the provision, to mean that the section does not generally apply to material which has been generated within the agency which holds it. However, this interpretation is not obvious in the wording of the section and might benefit from clarification in the legislation.

⁴⁰ Six submissions supported expanding the provision for withholding evaluative material - see submissions L9, L12, L13, L23, F20, F37. Four submissions would like to have it cut back in scope - submissions L14, L17, S2 and S42. Five submissions appear to support it as it is - submission L4, L7, L10, L19 and S36.

⁴¹ For instance, in relation to section 27(1)(b) which expressly articulates a fear that other governments or international organisations might cease to entrust information to New Zealand and section 29(1)(g)(ii) which is concerned with the prejudice of the supply of information to certain news organisations. Similar concerns exist, in relation to the protection of informant identity under section 27(i)(c) since future informants might not come forward if they could not be given an appropriately framed promise of confidentiality.

⁴² This will usually be someone outside the agency but may also, infrequently, include someone within the agency who is not obliged to give such information as part of the duties of his or her job. This latter situation arose in the *Westwood* case and the same result would arise under the proposal.

“WCC does not believe that 29(3) should be expanded and recommends a reduction.”

- WELLINGTON CITY COUNCIL,
SUBMISSION L14

**RECOMMENDATION 53**

It should be made clear that section 29(1)(b) is not available in relation to material that is provided by a person within the agency as part of his or her job.

Response to include grounds

- 4.4.16 There will remain cases where the evaluative material reason for refusing requests will continue to be applicable. Indeed, recommendation 53 will only affect a small proportion of the cases in which the reason is presently given.
- 4.4.17 Where evaluative material information is withheld by a public sector agency the resultant concern for the individual is usually mitigated by that person exercising a request under section 23 of the Official Information Act for reasons for the substantive decision. However, this is not available where a request is made of a private sector agency such as an employer or insurer.
- 4.4.18 I have given careful thought to whether there is some other means by which the needs of the individual might be better met while still protecting the interests of the agency. I have concluded that the agency should be obliged to provide a fuller response in refusing such a request than would normally be required by giving the requester both the reason for refusal and grounds in support. Normally an agency need only give the reason for refusal and a second request for the grounds is required under section 43(2)(b) or 44(a)(ii). The grounds will require a statement to be given of the considerations of fact, law and policy which led the agency to assign the reason for refusing the request in the particular case.
- 4.4.19 The grounds will have to be particularised for the case thereby ensuring that the agency carefully considers the statutory tests and the ability to withhold. The change may diminish the cases in which the reason is wrongly cited to brush-off a requester. It will also give the requester a better idea as to whether the information is properly withheld.

**RECOMMENDATION 54**

Sections 43 and 44 should be amended so that the grounds in support of the reasons for withholding evaluative material be given, without the requester needing to expressly ask, unless the giving of those grounds would itself prejudice the interests protected by section 29(1)(b).

Evaluative material held by author

- 4.4.20 At least upon first reading, section 29(1) seems to apply only to protect evaluative material in the hands of the recipient agency and not in the hands of its author. It may be that this was sufficient in the public sector under the Official Information Act when what was protected was material supplied by individuals or by private sector agencies, neither of which were subject to a right of access. The situation is different now with the extension of access into the private sector and it may seem odd if the provision did not allow the author of evaluative material to hold it back in circumstances where the recipient agency may do so.
- 4.4.21 Accordingly, in the discussion paper, I asked whether section 29(1)(b) should be revised to clarify that the author of evaluative material may withhold it from the subject in circumstances where the material may be withheld by the recipient agency. A good response was received to this question with 17 answers.⁴³ Every single one of them agreed that the provision should be so revised. The submission from the Ministry of Justice made the pertinent point that the issue would tend to arise only when the requester knew the identity of the supplier of the evaluative material - a detail frequently withheld. I have only occasionally seen the issue arise in practice in complaints to my office and I suspect that requesters have not yet worked out that where an agency withholds such mate-

“Sieghart made the pragmatic argument that the right of access ‘is a means rather than an end, because the end is to get the information system right, and if you give the data subject the right of access it is much more likely to be right’.”

- DAVID H FLAHERTY, *PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES*, 1989

⁴³ See submissions, L2, L4, L9, L10, L12, L13, L14, L17, L19, L22, S1, S2, S11, S13, S36, S37 and S42.



rial they might, through a process of deduction and multiple principle 6(1)(a) requests, identify who has supplied the information and request access to it.

- 4.4.22 In making the recommendation I acknowledge that the scope of this basis for withholding will be broadened which is a matter I have earlier expressed concern about. Nonetheless, if the basic shape of the evaluative material withholding provision is seen as reasonable and appropriate then I believe the case for protecting the information in the hands of the author is sound. Certainly those people who made submissions seemed to think so.



RECOMMENDATION 55

Section 29(1)(b) should be amended to clarify that the author of evaluative material may refuse an information privacy request in circumstances where the material may be withheld by the recipient agency.

29(1)(c): Physical or mental health

- 4.4.23 Section 29(1)(c) provides that an agency may refuse to disclose personal information relating to the requester’s physical or mental health if, after consultation (where practicable) with the individual’s medical practitioner, it is satisfied that disclosure of the information would be likely to prejudice the requester’s physical or mental health.

Use of provision

- 4.4.24 This withholding ground is not frequently relied upon by agencies and I have received few complaints. However, one unsuccessful complainant took such a matter to the Complaints Review Tribunal. In the case of *M v Ministry of Health*⁴⁴ the Tribunal gave consideration to the interpretation of the provision. One aspect related to the question of who is the “individual’s medical practitioner” when, as is common in these cases, the individual is receiving, or has received, treatment through the mental health system. The issue is whether the agency should consult the individual’s psychiatrist or general practitioner. The Tribunal took the view that it should be the “medical practitioner whose primary ethical obligation is to the individual” which it considered “most likely to be the requester’s general practitioner or the specialist with whom the requester has more than a passing patient/doctor relationship”.
- 4.4.25 There is a natural suspicion amongst patients, and individuals interested in information access issues, at suggestions that individuals ought not to be made aware of information about them because such knowledge would be likely to harm their health. Some worry at “doctor knows best” overtones which hark back to an era when individuals were generally not shown their medical records at all. However, in practice the withholding ground is relied upon in a very sparing manner. In the few cases that come for review the agencies, and medical practitioners involved, have usually done a great deal of soul searching before withholding the information. The concerns for physical or mental health are genuinely held and agencies often believe that the consequences of disclosure can be dire indeed. Provision for independent review also helps ensure that potential misuse of the ground is minimised. Some health agencies offer the availability of a counsellor or doctor to discuss concerns at the contents of documents revealed in order to minimise the risks consequent upon disclosure.

Psychologists

- 4.4.26 I received an unsolicited submission from a clinical psychologist who suggested that the present reference to an individual’s medical practitioner in section 29(1)(d) be replaced by one which would include an individual’s psychologist. Two scenarios were outlined. The first would involve a request directly to a psychologist. The submission was that the psychologist should be able to with-

⁴⁴ (1997) 4 HRNZ 79.

hold information under the provision without the need to consult with the individual's medical practitioner. The second suggestion was that other agencies holding information be permitted to consult with the individual's psychologist as an alternative to consulting the individual's medical practitioner.

- 4.4.27 I do not accept the case made in the submission to permit psychologists to dispense with consultation with an individual's medical practitioner before withholding information under section 29(1)(c). The withholding ground is directed towards "physical or mental health". "Physical health" is the province of medical practitioners. "Mental health" is also primarily the province of medicine although a psychologist may also possess relevant knowledge and insights. In the rare cases where the issue arises, a psychologist may be better informed to make the decision to withhold information having spoken to the individual's medical practitioner.
- 4.4.28 However, there may be merit in the suggestion to allow for consultation with an individual's psychologist in assisting to determine whether information should be withheld. The issue will arise rarely since practically all New Zealanders have someone they consider "their doctor" whereas few would say so in relation to a psychologist. However, in those circumstances where an agency proposes to withhold information and knows that the individual has a psychologist it does not seem unreasonable that that person be consulted as an alternative to the individual's medical practitioner in appropriate cases.
- 4.4.29 Alberta appears to be the only jurisdiction which has provided an explicit role for psychologists. Section 17(2) of the Freedom of Information and Protection of Privacy Act 1994 (Alberta) states:

"The head of a public body may refuse to disclose to an applicant personal information about the applicant if, in the opinion of a physician, a chartered psychologist or a psychiatrist or any other appropriate expert depending on the circumstances of the case, if disclosure could reasonably be expected to result in immediate and grave harm to the applicant's health or safety."

- 4.4.30 It is important in my view that the emphasis remain on consultation being with the *individual's* medical practitioner or psychologist not, as in the Alberta provision, just any practitioner. I am not proposing that agencies should seek a specialist opinion from a psychologist for the purpose of sustaining the withholding of information. It is simply that if the individual already has a relationship with a psychologist then it may be appropriate in some circumstances to consult that person rather than the individual's medical practitioner. It remains open to the agency to consult both the psychologist and doctor.
- 4.4.31 As I have received a submission from only one practitioner I couch my recommendation as a matter for further consideration.



RECOMMENDATION 56

Consideration should be given to amending section 29(1)(c) to provide for consultation with the individual's medical practitioner or, in the circumstances of the case, the individual's psychologist.

29(1)(d): Young persons

- 4.4.32 The Act permits refusal of a request in the case of an individual under the age of 16, where the disclosure of the requested information would be contrary to that individual's interests.
- 4.4.33 The provision has been carried over into the Act from section 27(1)(e) of the

Official Information Act although it was not included in the draft bill prepared by the Danks Committee.⁴⁵ That provision has been described as:

“A paternalistic but somewhat vague injunction not to release information.”⁴⁶

4.4.34 The withholding ground might arise in two slightly different circumstances. The first would concern a request for information by an individual under the age of 16 for information about him or herself the disclosure of which would be contrary to that individual’s interests. It is in this context that the ground is sometimes called paternalistic and in that respect it has something in common with the previous withholding ground whereby information can be withheld to protect the physical or mental health of an individual. However, the provision also has relevance to the circumstances where another person seeks access to information which is personal information about both the requester and a person under the age of 16. In that case, the requester can be denied information where disclosure would be contrary to the young person’s interests.

4.4.35 Notwithstanding that I received few complaints concerning refusal of requests based upon section 29(1)(d), a case has already been to the Complaints Review Tribunal in relation to it. In *O v N (No.2)*⁴⁷ the Tribunal held that the standard of proof implied by the expression “would” in the provision was the balance of probability. The Tribunal also surmised whether the “interests” of the child in section 29(1)(d) meant “best interests” - a phrase frequently used in family law. In particular, the Tribunal noted that article 3(1) of the United Nations Convention on the Rights of the Child it provides that:

“In all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, the best interests of the child shall be a primary consideration.”

4.4.36 The Tribunal suggested that section 29(1)(d) might be considered to give effect to the Convention and that “interests” might denote “best interests” to accord with New Zealand’s international obligations. However, the issue was left open. I consider that little turns on the issue but that if it did, the Tribunal would likely interpret the meaning to be “best interests”. I do not consider it necessary to amend the provision.

29(1)(e): Safe custody or rehabilitation

4.4.37 Section 29(1)(e) provides that an agency may refuse to disclose information in respect of an individual who has been convicted of an offence or detained in custody where it would be likely to prejudice that individual’s safe custody or rehabilitation. The provision is derived from the Official Information Act and was included in the Danks Committee proposals.⁴⁸

4.4.38 The provision has been considered by the Complaints Review Tribunal in *M v Police*.⁴⁹ Interestingly, although the case mainly turned on prejudice to custody, although rehabilitation was cited, the requester was not in actual custody when the decision was made to withhold the information. Instead he had been released on licence but able to be recalled into custody. Nonetheless, the Tribunal took a relatively robust approach and concluded that this amounted to much the same thing as custody and allowed the withholding of the informa-

⁴⁵ Committee on Official Information, *Towards Open Government: Supplementary Report*, 1981.

⁴⁶ *Freedom of Information in New Zealand*, 1992, page 538.

⁴⁷ (1996) 3 HRNZ 636.

⁴⁸ See Committee on Official Information, *Towards Open Government: Supplementary Report*, page 80.

⁴⁹ (1997) 4 HRNZ 91.

tion on the basis that it would prejudice the requester’s safe custody or rehabilitation. I have no recommendation for amendment.

29(1)(f): Legal professional privilege

- 4.4.39 Section 29(1)(f) provides that an agency may refuse to disclose information where disclosure would breach legal professional privilege.
- 4.4.40 “Privilege” is a term borrowed from the common law and statutory rules about which evidence could be sought and given in court proceedings. The concept was developed before individuals had a right of access to personal information about themselves. Legal professional privilege protects certain communications between clients and their legal advisers and, if litigation is in prospect, communications with third parties for the purpose of that litigation. The law protecting legal privilege is not as wide as members of the public might think.
- 4.4.41 A problem did arise during the period under review when certain agencies withheld information on this ground but were reluctant to provide the documentation to the Commissioner on investigation of the resulting complaints. This issue was resolved to my satisfaction with an amendment to section 94 of the Act, as discussed at paragraphs 9.6.2 - 9.6.6.
- 4.4.42 “Legal professional privilege” is a concept understood by lawyers but not necessarily well understood by their client agencies or by requesters. It would be desirable to present the provision in a more informative fashion if that is possible. A recent review of the Australian Freedom of Information Act recommended that the relevant reason for refusal should contain an explanation of the common law of legal professional privilege. It was considered that this would effectively make the ground self-contained and thus easier for requesters and agencies to understand. Accordingly, it was recommended that the relevant section:
- “Should be redrafted to provide that a document is exempt if it was created for the sole purpose of:
(i) seeking or providing legal advice; or
(ii) use in legal proceedings.”⁵⁰
- 4.4.43 Such a provision in New Zealand might refer to the “dominant” rather than “sole” purpose. At the present time the law of evidence is under review by the Law Commission which may make some further change in this respect. I have no wish to express a view as to what the extent of legal professional privilege ought to be, merely that it would be desirable to have its elements spelt out directly in the reason for withholding.



RECOMMENDATION 57

Section 29(1)(f) should be redrafted so that it provides a self-contained explanation of the meaning of legal professional privilege.

- 4.4.44 There has been some discussion in this review, and in the Law Commission’s review of the law of evidence, as to whether a kind of legal professional privilege should be able to be asserted where the relevant communications, do not involve a barrister and solicitor but some other kind of legal adviser or advocate. In particular it has arisen in the context of industrial advocates employed by School Boards of Trustees. It seems to me that the present position could be considered anomalous but I suggest that the matter be resolved through the reform of evidence law following the Law Commission’s report. The key issue to be addressed is the appropriate scope of privilege - not a matter determined

⁵⁰ Australian Law Reform Commission and Administrative Review Council, *Open Government: A Review of the Federal Freedom of Information Act 1982*, 1995, page 138.

by the Privacy Act but by the Law of Evidence. If any change is adopted there it will be followed in the reasons for withholding.

29(1)(g): Radio NZ Ltd/TVNZ Ltd

4.4.45 The information privacy principles generally do not apply to the news media. This is achieved by excluding any “news medium” in relation to its “news activities” from the definition of “agency”. Clearly both Radio New Zealand Ltd and Television New Zealand Ltd are each a “news medium”. However, the definition of that term in section 2 expressly excludes Radio New Zealand Ltd and TVNZ in relation to principles 6 and 7. Therefore they are agencies for the purposes of those principles.

4.4.46 This arrangement reflects the fact that as public sector organisations these two entities had been subject, since 1982, to the personal information access and correction regime then provided for in the Official Information Act and which is now reflected in principle 6 and 7. When this access regime was transferred to the Privacy Act it was considered important not to reduce those access and correction rights simply by reason of the transfer.

Restructuring of RNZ

4.4.47 One development during the period under the review concerned the restructuring of Radio New Zealand with a view to retaining Radio New Zealand Ltd as a Crown entity but separating the commercial operations to enable their possible sale - which also eventuated during the period. The Radio New Zealand Act (No 2) 1995 achieved this by deleting the words “Radio New Zealand Limited” and substituting the words “Radio New Zealand Ltd, The Radio Company Ltd, or”. This change was effected from the date that that Act commenced and, at a later date when the company was sold, a further amendment took effect which omitted the reference to “The Radio Company Ltd”.

4.4.48 I did not oppose the amendments to the Privacy Act.⁵¹ The first amendment simply reflected the restructured organisation and did not in any sense change the existing application of the Privacy Act. Similarly, when the privatisation was complete and the second amendment took effect, the application of the Privacy Act has still not in any real sense changed. From the time that the commercial part of Radio New Zealand was sold, the news activities of that commercial company were placed in exactly the same position as every other private radio broadcaster. Accordingly, while the personal information access rights in relation to the commercial part of RNZ diminished somewhat the fundamental position under the Privacy Act remained the same with respect to the exemption of the news media in their news activities.

Protection of sources

4.4.49 Complaints against Radio New Zealand and TVNZ are infrequent. Where such complaints are made they usually fall foul of the news media exemption. I have not released any case notes concerning the position of RNZ, TVNZ or the application of section 29(1)(g).

4.4.50 The two state broadcasters remain subject to the access and correction regime. Section 29(1)(g) has been crafted to ensure that *bona fide* news media journalists can protect their sources by withholding information where either:

- the information is subject to an obligation of confidence; or
- the disclosure of the information would be likely to prejudice the supply of similar information, or information from the same source.

4.4.51 I can anticipate circumstances in which I would need to investigate a complaint about the withholding of information against TVNZ or RNZ where it is neces-

⁵¹ See Report of the Privacy Commissioner to the Minister of Justice on the Radio New Zealand Bill, 10 July 1995.

sary to question a journalist as to whether information is subject to an obligation of confidence. I am aware from other dealings during the period under review, where enquiries have needed to be made of news organisations or journalists, that there is some misunderstanding about the manner in which such complaints can be dealt with. It is a delicate area which involves the balancing of important public and private interests. However, such balancing is “the bread and butter” of a Privacy Commissioner whose role is to investigate and resolve privacy complaints.

- 4.4.52 There is a mistaken belief in some quarters that it is somehow improper even to ask a journalist as to whether information is held or whether that information is subject to an obligation of confidence or is necessary to be withheld to protect sources of information. Quite clearly to do my job of investigating complaints these questions must sometimes be asked. It is no threat to press freedom to simply pose such questions. It is open for the journalist, in appropriate cases, to assert that the information held is subject to an obligation of confidence or that sources of information would be jeopardised if the information were to be released. However, journalists receive information from a whole variety of sources and the release of such information will not in all, or even necessarily most, cases jeopardise such sources. An example would be where information is obtained from a public source or pursuant to an Official Information Act request. There may also be cases where the matter can be resolved by asking the source of information. If they do object it may well be necessary to withhold the information to protect the confidential information. Where no objection is taken it may well be possible to release the information requested.
- 4.4.53 It is clearly in the public interest to have a free and fearless news media. However, this is not under threat in New Zealand from the access provisions of the Privacy Act and it is ridiculous to suggest that it is placed in jeopardy by questioning by the Privacy Commissioner to see whether a withholding ground applies. It is incumbent on the news media in my opinion to ensure that the cherished reputation of the “fourth estate” is upheld through professional and ethical conduct. This does not permit the hiding of sources of information in every case - sometimes it is essential to know the source of information to assess the credibility of material published. In many cases, it is as much a part of proper journalism to *reveal* sources, as it is to protect them, if the public is to have faith in what is published. Any move to make the position more difficult will only hamper my investigations. Approaches by my office to journalists seem to be met with less than a measured and considered reaction by newspapers with, in one case, use of news columns to castigate my approach before I had even reached the stage of deciding to require a response to a question as to the source.

Access, correction and the news media

- 4.4.54 Section 29(1)(g) is modelled on a provision which has appeared in the Official Information Act. It has operated, so far as I am aware, without any particular difficulty. An argument could be mounted to say that the complete exemption from the access and correction regime enjoyed by other news media organisations may not be warranted if any rights were accompanied with an appropriately crafted withholding ground such as section 29(1)(g).
- 4.4.55 A number of European laws have applied their access and correction regimes to the news media (sometimes only in respect of published material). While I do not believe that proposition should be rejected out of hand, I do not recommend such a course in this review. However, it would be desirable, in my view, for news media organisations singularly or collectively to consider whether some sort of entitlements could be provided to individuals on a self-regulatory basis. I note that some newspapers now have Internet sites on which it is possible to search a name. It does not therefore appear to be contrary to any fundamental freedom of such concept to be able to access information published about one-

self if it is reasonably retrievable for the publication. To be credible, there would need to be some kind of scrutiny external to the journalist concerned where information is withheld. This would not necessarily have to be an industry ombudsman, or a complaints body such as the Press Council, but might be in the form of, say, an organisation's ethical reviewer. Possibly that role could appropriately be held by an agency's privacy officer.

29(1)(h): Library, museum or archive

4.4.56 Under the Privacy Act there is a right of access to personal information contained in a library or museum. Such information is available as personal information except where the disclosure of it would be in a breach of a condition under which the material was placed in the institution.

4.4.57 I am unaware of any problems with this provision in operation and do not recommend change at this time.

29(1)(i): Contempt of court or Parliament

4.4.58 As with the Official Information Act, cases concerning the withholding of information on the grounds that the disclosure would constitute contempt of court or of the House of Representatives are very rare.

4.4.59 Although the reason for refusal is derived from the Official Information Act there was, in fact, no such withholding ground for personal information requests under Part V of the Official Information Act.⁵² Dr Roth has observed that the position taken under the Privacy Act “is more straightforward” than under the Official Information Act.⁵³ In particular, there is no provision in the Privacy Act which has the effect of placing a decision to disclose personal information outside the protection of the legislation's immunities as, Dr Roth advises, section 52(1) of the Official Information Act does. In particular, if personal information is disclosed in good faith pursuant to principle 6, and it does constitute contempt, the agency involved will enjoy the protection afforded by section 115 of the Act in respect of contempt of court proceedings.

4.4.60 I am unaware of any particular problems with this provision and have no recommendations for change.

29(1)(j): Frivolous, vexatious or trivial

4.4.61 Section 29(1)(j) provides that an agency may refuse disclosure where the request is frivolous or vexatious or the information requested is trivial.

4.4.62 The first part of the reason for withholding relates to the *request*. This allows for refusal where a request is frivolous or vexatious.

4.4.63 The second part of the paragraph relates to the *information*. This allows for refusal of a request where the information requested is trivial.

4.4.64 The provision has been carried over from section 27(1)(h) of the Official Information Act. The “frivolous or vexatious” ground is directed towards a request which is an abuse of the procedure and not bona fide. Essentially the requester is abusing the rights granted by the statute rather than exercising those rights as intended. The ground is hardly ever relied upon, certainly not in cases which have been brought on review to me. There may be many reasons for this. Perhaps requesters are careful not to misuse the access rights that have been

⁵² Under section 18(c)(ii) contempt of court or of the House of Representatives constitutes a reason for refusal of Part II requests under the Official Information Act and section 52(1) makes it clear that Act does not authorise or permit the making available of any official information if that would constitute a contempt of court or of the House of Representatives.

⁵³ *Privacy Law & Practice*, paragraph 1029.22.

granted to them. Perhaps agencies grant access and avoid a complaint notwithstanding occasional abuse of the rights. Probably on the occasions where resort might be had to the provision, agencies are reluctant to use it because they are unable to show that there was a vexatious intent. Such an intent may be difficult to prove if the requester has expressed no motive for a request.

- 4.4.65 Similarly, it appears that agencies very rarely rely upon the trivial information ground to refuse access to information. Often it is easier to simply give access to a trivial information than to refuse it on this ground and incur customer or employee displeasure and the possibility of a complaint. With respect to private sector agencies, the ability to charge for the information may filter out, or compensate for, the odd trivial request that might be received.
- 4.4.66 Elsewhere I have recommended a provision enabling an agency to apply for an exemption from having to deal with a named individual's access request for a fixed period where it can be shown that the individual has lodged requests of a repetitious or systematic nature which would unreasonably interfere with the operations of the agency and amount to an abuse of the right of access.⁵⁴ Clearly this has some similarity to the frivolous or vexatious ground for refusing requests. However, the proposal does not precisely replicate the existing provision and may add a safeguard in the very rare cases where this problem arises. That proposal would place an emphasis on the *systematic or repetitious* lodging of requests whereas the existing ground for refusal is directed towards a particular request (although a pattern of requests might give grounds to infer something of the requester's motives). It would also allow an agency to disregard, for a period, requests from the person who has systematically abused the right of access without needing to deal with each request on a case by case basis.
- 4.4.67 The Complaints Review Tribunal has the power to dismiss *any* proceedings (not simply access proceedings) if it is satisfied that they are trivial, frivolous, or vexatious or are not brought in good faith.⁵⁵ I have similar discretion to decline to investigate complaints under section 71(1)(c).

29(2): Unavailability of information

- 4.4.68 Section 29(2) sets out what have been called “administrative reasons” for not granting a request for personal information pursuant to principle 6. An agency may refuse a request where the information is not readily retrievable, does not exist or cannot be found, or where it is not held by an agency, and the person dealing with the request has no grounds for believing that the request can be transferred to another agency.
- 4.4.69 The reasons for refusal of requests under section 29(2) are reasonably plain and easy to understand and apply in practice. However, they each give rise to conceptual difficulties and the need for the provisions, or at least some of them, has been called into question. For example, Dr Paul Roth has suggested that paragraphs (b) and (c) “appear to serve no practical purpose”.⁵⁶ Recently the Law Commission completed a study of the equivalent administrative reasons for refusing requests under the Official Information Act and its report, although not recommending change, highlighted a series of legal complexities in what one might have expected to be a relatively straightforward aspect of information law.⁵⁷

29(2)(a): Not readily retrievable

- 4.4.70 It is not immediately apparent why section 29(2)(a) is needed since it merely reproduces part of the precondition for entitlement to access personal informa-

⁵⁴ See recommendation 66.

⁵⁵ See Privacy Act, section 89 and Human Rights Act, section 115.

⁵⁶ *Privacy Law & Practice*, paragraph 1029.25.

⁵⁷ Law Commission, *Review of the Official Information Act 1982*, chapter 8.

tion under principle 6(1) - that personal information must be held “in such a way that it can readily be retrieved”.

4.4.71 Had there been no section 29(2)(a) an agency could still refuse a request because of the limitation of the entitlement under principle 6. Similarly, an agency might refuse a request for any of the following reasons notwithstanding that they are not set out as specific reasons for refusal:

- the request is not made by or on behalf of the individual concerned;
- the request is not for “personal information” but for information about a corporate body or some other thing;
- the request is made by a person who does not have standing under section 34.

4.4.72 Nonetheless, the existence of the withholding ground probably makes for a more workable access process since the agency has a ready reason to refuse the request and the requester gets a clear answer. Otherwise agencies who are perhaps not familiar with the Act, and who merely look through the list of withholding grounds, might fail to notice that they need not make the information available or may have to devise an appropriate response. From the requester’s point of view they will get a clear reply to their request notwithstanding that their request arguably does not constitute an “information privacy request” as falling outside their entitlements under principle 6 (although of course the requester would not have known that). Where individuals know, or believe, that information is held by an agency it is desirable that they receive a response making it clear that the information is “not readily retrievable” so that they may have the opportunity to discuss with the agency what information might be retrievable.

4.4.73 The withholding ground does appear anomalous notwithstanding that it has not caused any real problems in practice and is usefully listed amongst the reasons for refusing requests. One way of removing the anomaly would be to delete section 29(2)(a). This would bring disadvantages in terms of the orderly processing of access requests, the providing of responses, and the availability of review. The other, more promising, way of removing the anomaly would be to omit the “readily retrievable” condition precedent to the access right in information privacy principle 6(1) itself. This would have the effect of removing any redundancy without reducing individual rights. If change were to be made I would prefer this approach. However, I do not presently recommend change.

29(2)(b): Information requested does not exist or cannot be found

4.4.74 It has been suggested that paragraph (b) appears to serve no practical purpose in that information which does not exist or cannot be found can also be considered to be “not readily retrievable” in terms of paragraph (a) or not information held in such a way that it can readily be retrieved in terms of principle 6(1).

4.4.75 However, the prevailing view appears to be that information which is not readily retrievable may nonetheless exist and may be able to be found.⁵⁸ This was illustrated in the case of *Mitchell v Police Commissioner*.⁵⁹ In that case, the information, consisting of four affidavits, would have been returned by the person who physically held them if the defendant, who had the authority to ask for their return, had so requested. The defendant’s evidence indicated that the affidavits were not retrieved because it was not known where they were. The Tribunal stated that this explained why the affidavits were not retrieved but did not alter the fact that they were retrievable. The Tribunal also took the view that it is implicit in the phrase “cannot be found” that reasonable attempts have been made to find the information otherwise an agency making no attempt to

⁵⁸ See Law Commission, *Review of the Official Information Act 1982*, paragraph 292.

⁵⁹ [1985] NZAR 274.

find information, or only a desultory attempt, would be justified in refusing a request and the objective of the legislation would be thwarted.

- 4.4.76 While conceptually it is possible to take a position that paragraph (b) is not needed because it is implicit in the “readily retrievable” provisions I nonetheless support its retention. Even if implicit, the “does not exist” or “cannot be found” provision is more precise and provides a useful explanation to the requester when a refusal is made. The reason offers a guide to investigating the matter if a complaint is lodged. If information is refused for this reason, and a complaint is investigated, a primary line of enquiry will be the nature and quality of the searches made. The same could not be said of all “not readily retrievable” cases.

29(2)(c): Requested information is not held

- 4.4.77 The first part of paragraph (c) repeats a precondition for entitlement to access to personal information under principle 6(1), which entitles an individual to access only “where an agency holds personal information”.
- 4.4.78 Accordingly, as with paragraph (a), it might be argued that the reason for refusal is not necessary. Nonetheless, as with paragraph (a), there is probably merit in retaining the provision. The ground for refusal is useful when a request is broadly framed and only part of the information requested is held by the agency. The information that the agency does hold is readily retrievable but the balance of the information would be refused under this provision.
- 4.4.79 The ground for refusing a request has a second part which is that the person dealing with the request also has no grounds for believing that the information is either held by another agency or connected more closely with the functions or activities of another agency. Although the provision does not say so, the language seems clearly indicated to link to section 39 which concerns transfer of requests. It seems to be contemplated that such requests not be met with an outright refusal but instead a response informing the individual as to the transfer. However, this link is not very plain and would no doubt confuse some agencies unfamiliar with the provisions who may be perplexed, for example, as to why a request for information that is not held by the agency cannot be refused.
- 4.4.80 It might be preferable to redraft paragraph (c) to make the link with the transfer provision plainer. Something along the lines of the following might suffice:

“The information requested is not held by the agency and the person dealing with the request has no grounds for believing that the request should be transferred to another agency under section 39.”



RECOMMENDATION 58

Section 29(2)(c) should be redrafted to make plain the link with the obligations to transfer a request.

29(3): Evaluative material

- 4.4.81 Subsection (3) contains a definition of “evaluative material” which has been derived from the Official Information Act. I have discussed the refusal of requests for evaluative material in relation to section 29(1)(b) and made some recommendations for change.⁶⁰ I have also canvassed elsewhere the possibility that if the grounds for withholding were to be reorganised the provisions relating to evaluative material might be better located in conjunction with other provisions dealing with commercial and related interests.⁶¹

⁶⁰ See paragraphs 4.4.13 - 4.4.22 and recommendations 53, 54 and 55.

⁶¹ See paragraph 4.3.11.

4.5 SECTION 30 - Refusal not permitted for any other reason

4.5.1 Section 30 indicates that the good reasons for refusing disclosure, set out in sections 27, 28 and 29, are intended to form a code. In other words, no reasons other than one or more of those set out in those sections justifies a refusal to disclose information requested pursuant to information privacy principle 6. This is subject to three sections:

- section 7 - which saves the effect of other laws;⁶²
- section 31 - which has never been brought into effect, but were it to be, would place restrictions on persons sentenced to imprisonment; and
- section 32 - which allows an agency to “neither confirm nor deny” the existence of certain information.

Counselling and medical privileges

4.5.2 In the course of this review consideration was given to whether there ought to be any new reasons for refusal of requests created. Most submissions felt that there should be no further reasons for refusal.⁶³ However, drawing upon the analogy with legal professional privilege, suggestions were directed to other forms of privilege, such as counselling communications, which have certain limited privileges under the Evidence Act.⁶⁴ Privilege involving medical practitioners was also raised.⁶⁵ Such “privileged” information is frequently able to be withheld under section 29(1)(a) because its release would involve the unwarranted disclosure of the affairs of another individual. However, without a more tailored reason for refusal the matter has to be gone into on a case by case basis by the agency, and on review by my office and the Tribunal, and documents cannot be withheld on a class basis in the same way as communications which are subject to legal professional privilege.

4.5.3 For example, it is not unknown for persons who have been charged with, or convicted of, certain sexual offending to seek access to information which is held on the ACC counselling files of victims or alleged victims. Nearly all of this information is withheld on the basis that it is not in fact personal information about the requester. However, where it is mixed information about the requester and the person undergoing counselling, a careful process has to be gone into to identify in detail what is personal information about the requester and, of that, what can be withheld. These issues also arose when the access regime was solely within the Official Information Act. The new feature is that private sector agencies, such as counselling organisations and GPs, are now subject to the access regime.

4.5.4 This raises a question of competing privacy interests. There is very high privacy interest in the person who has consulted a doctor, or undergone counselling, and disclosed information in confidence. Against that is the privacy interest in a requester having access to a portion of the information that relates to him or her. The interest in having confidences respected in professional consultations or counselling may have more importance than the desire on the part of the requester to have access to what has been said about him or her. After all, generally speaking, what an individual discloses in counselling sessions, or in medical consultations, is not used in relation to the requester - it is a matter between individual and professional.

4.5.5 However, there are some classes of case where what is said in confidence may have a direct bearing upon actions taken in relation to the requester, particu-

“The medical (patient-doctor) privilege appears to be disregarded more than recognised. While there are exceptions to such privilege where disclosure is needed to prevent harm, I believe the doctor’s professional privilege should be no less respected than the lawyer’s. Counsellors would, no doubt, argue similarly. I expect there to be more harm resulting from disclosure than protection of confidence.”

- ROYAL NZ COLLEGE OF GENERAL PRACTITIONERS, SUBMISSION L4

⁶² I suggest elsewhere that relevant parts of section 7(2) and 7(3) should be transferred into Part IV itself. See recommendation 32.

⁶³ See submissions L7, L9, L13, L14, L19 and L22.

⁶⁴ See submissions L18 and L24.

⁶⁵ See submissions L4 and S2.

larly in relation to criminal proceedings. There are currently proposals to establish a criminal disclosure regime which may resolve a significant aspect of the problem with respect to persons who have been charged with an offence. If such a regime is established the case to include counselling or medical privilege would, I believe, be significantly strengthened since in such cases relevant information will be available, if appropriate, through court supervised processes without any need to rely upon Privacy Act access rights.

4.5.6 Although there may be merit in addressing the matter, I do not think that the time is right. Very shortly a major review of the law of evidence will be examined by the Government. Similarly, a proposal for a criminal discovery regime seems imminent after a wait of many years (see paragraphs 4.6.1 - 4.6.5). The possibility of creating any new withholding grounds may more appropriately be considered once the details of those two initiatives are known.

4. 6 SECTION 31 - Restriction when person sentenced to imprisonment

4.6.1 For some years there has been discussion of creating a criminal discovery procedure, that is, a formal means for defence and prosecution counsel to exchange information about a criminal case. In the absence of a statutory discovery procedure the Courts may make decisions under the Privacy Act and Official Information Act.

4.6.2 Once a criminal discovery procedure is enacted, section 31 may be brought into effect. Section 31 would allow the police to refuse a request for information relating to an offence where the person concerned has already been convicted for that offence. The section comes from the Official Information Act where it was introduced in 1987. It is waiting to be enacted by an Order in Council, as it was when it was in the Official Information Act.

4.6.3 In October 1997 the Ministry of Justice and Department for Courts began consulting in relation to a proposal regarding preliminary hearings and criminal disclosure. I have supported the creation of a statutory criminal discovery or criminal disclosure regime and in most major respects the detail of the joint position taken by the Ministry and the Department.⁶⁶ In my view the Privacy Act does not provide an ideal basis for a criminal disclosure regime although the position may be better than it is in common law regimes without such legislation. The consultation paper issued by the Ministry and Department raised the issue of whether section 31 of the Act should come into effect.

4.6.4 The consultation paper noted that reform of disclosure in Britain was precipitated by a series of high profile criminal convictions being overturned, some years later, on the grounds that the prosecution had failed to disclose certain evidence that would have been helpful to the defendant. The information only came to light by the defendant's continuing to seek disclosure after the trial had been completed. Given human fallibility - not to mention the possibility of improper behaviour - we should not always assume complete and perfect compliance with disclosure obligations.

4.6.5 It is not possible for me to know how the departmental proposals will develop and at what pace. In my view, section 31 should be repealed regardless of the outcome of that initiative.



RECOMMENDATION 59

Section 31 should be repealed.

⁶⁶ See submission by the Privacy Commissioner to the Ministry of Justice and Department for Courts in relation to the consultation paper regarding preliminary hearings and criminal disclosure, February 1998.

4.7 SECTION 32 - Information concerning existence of certain information

- 4.7.1 Section 32 allows agencies to respond for requests to access by neither confirming nor denying the existence or non-existence of the information in question. The provision is quite tightly drawn and only permits such a response where section 27 or 28 of the Act is being relied upon - that is primarily in cases involving national security or law enforcement and less frequently cases involving personal safety or international relations.
- 4.7.2 The provision is derived from section 10 of the Official Information Act and the issues arise far more frequently in that context. I have occasionally had to consider such matters especially in the context of access complaints involving the New Zealand Security Intelligence Service.⁶⁷
- 4.7.3 Section 10 of the Official Information Act was not one of the provisions considered by the Law Commission in its review of the Official Information Act. However, a similar provision was considered in a recent review of the Australian Freedom of Information Act. In the report of that review it stated that the equivalent section, section 25:

“... is especially problematic for applicants because it appears to perpetuate the kind of secretive, conspiratorial agency culture that the FOI Act is intended to break down. DP59 asked whether there is a problem with the ‘neither nor confirm’ response provided for s.25. A number of submissions consider that s.25 is contrary to the spirit of the Act and should be repealed. Others consider it a necessary provision.

“The review is concerned that s.25 can be used ‘bamboozle’ applicants with legalistic jargon. Nevertheless it considers that, unfortunately, provision is necessary where information about the existence (or non-existence) of a document needs to be withheld. However, reliance on s.25 will only be justified in rare situations.”⁶⁸

- 4.7.4 The Australian review recommended that the grounds upon which the neither confirm nor deny response could be made should be slightly narrowed (in circumstances not relevant to this review). I agree that it is necessary to have such a provision in an access law. I also take the view that a “neither confirm nor deny” response should only be justified in rare situations.

Broadening the application of section 32

- 4.7.5 However, it may be appropriate to consider whether the existing range of circumstances for which a neither confirm nor deny response can be given under section 32 is appropriate. Presently, there is broad brush approach applying the provision to circumstances in which section 27 or 28 apply (or would apply if the information exists). It cannot be utilised in respect of section 29. I consider that the reasons set out in sections 27 and 28(1)(b) are appropriate. It is perhaps not quite so clear that the provision has relevance to section 28(1)(a) but refusal on that ground is so rare that the issue probably has never arisen.
- 4.7.6 Notwithstanding my general wish that the “neither nor confirm nor deny” response should be available in limited circumstances, and utilised only rarely, it

⁶⁷ See, for example, case note 63W.

⁶⁸ Australian Law Reform Commission and Administrative Review Council, *Open Government: A Review of the Federal Freedom of Information Act 1982, 1995*, paragraphs 8.21 and 8.22.

occurs to me that there may be another circumstance in which the section 33 response should be available. Section 29(1)(e) concerns the disclosure of information which would be likely to prejudice the safe custody or rehabilitation of a convicted individual detained in custody. This provision is very similar to that contained in section 27(1)(c) concerning prejudice to the maintenance of the law. Overseas access laws that have a “neither confirm nor deny” provision for law enforcement reasons also permit such a response where disclosure might facilitate the escape from custody of a detained person.⁶⁹

- 4.7.7 At this time I merely raise the issue for consideration since it might appropriately be considered in conjunction with a review of the equivalent provision in the Official Information Act also. Any change to this provision would also have to be reflected in a change to section 44(a)(ii) which allows an agency to refuse to give grounds in support of reasons for refusal of access in certain circumstances.



RECOMMENDATION 60

Consideration should be given to extending the application of section 32 to information to which section 29(1)(e) applies.

⁶⁹ See, for example, Freedom of Information and Protection of Privacy Act 1992 (British Columbia), sections 8(2)(a) and 15.

Part V

V

Procedural Provisions Relating to Access to and Correction of Personal Information

175

“The amount of difficulty and expense involved in providing access to personal information will vary from case to case and cannot be known in advance. The matter should remain discretionary with, as at present, the possibility of a complaint should charges be considered unreasonable.”

- NZ Employers Federation, submission G10

“We have difficulties with the idea of charging for access to government information in an overall sense. Over the last several years now government agencies of all sorts have increased or introduced charges for information. We believe that unless carefully controlled and monitored and unless this type of charging is kept to the absolute minimum that this is bad for our democracy.”

- Commonwealth Press Union, submission G17

“We would not be happy for there to be included in the Privacy Act a blanket provision allowing a parent, or guardian of anyone under 16 to make a request on their behalf.”

- Commissioner for Children, submission L3

“We believe that personal information held by a public or private enterprise agency should be available for verification, free of charge, to the individual to whom that information relates.”

- Consumers’ Institute, submission L13

5.1 INTRODUCTION

- 5.1.1 Part V describes procedures that agencies must follow in dealing with requests for access to information under the Act or for correction of information held. The provisions are modelled on Parts II and IV of the Official Information Act 1982. They deal with such matters as who may make requests for access to information, the circumstances in which agencies may or may not charge for the provision of information, the obligation on agencies to provide assistance to individuals who wish to exercise their rights to request access to information and the manner in which information is to be made available.
- 5.1.2 There is considerable experience in relation to the procedural provisions for giving access to personal information. The provisions have been tested for many years in the Official Information Act and the Local Government Official Information and Meetings Act. It has been possible to draw heavily upon that experience in the operation of the Act over the last few years and in this review. A number of local and central government officers have shared their experience with me over the years. I have also benefited from my contact with the Ombudsmen over the period, and during this review, with staff who have been familiar with the provisions of the official information legislation or who have worked in the Ombudsmen's office, and in the published works on the official information legislation, such as the major work *Freedom of Information in New Zealand*.¹ I have also benefited from the publication of the Law Commission's *Review of the Official Information Act 1982* during the period of my own review.²
- 5.1.3 Unlike some of the novel, unusual, technical or even obscure, issues that I have dealt with elsewhere in the review, there is a wide body of experience amongst agencies themselves in working with the procedural provisions of Part V. Accordingly, I have welcomed a large number of submissions from agencies and privacy officers who work with the Act on this part of the review.³
- 5.1.4 The procedural provisions in Part V have, by and large, worked well. They closely follow provisions which were originally recommended by the Committee on Official Information (the "Danks Committee") although with some subsequent revision particularly in 1982 and 1987. While the Danks Committee undertook significant pioneering work, it was able to draw upon some earlier models in establishing these procedural provisions such as, in New Zealand, the Wanganui Computer Centre Act 1976 and, overseas, the USA legislation and an Australian bill. Useful precedents were also found in the Ombudsmen legislation, and other laws such as the Race Relations Act, in crafting provisions such as those dealing with frivolous or vexatious complaints.
- 5.1.5 However, other than the recent and relatively narrowly focused review by the Law Commission, there has been little systematic review of the procedural provisions in our information laws since 1987. While many of the changes I recommend for consideration in this area may be relatively minor I believe that they will contribute to a more effective and efficient access law. I am keen to preserve and enhance the many informal and straightforward mechanisms provided for in the Act, and modelled upon the earlier official information and Ombudsmen legislation. In this regard, our laws contrast with certain overseas freedom of information and access laws which sometimes call for an excessive degree of formality in the making and processing of access requests. I believe that the New Zealand approach also helps minimise compliance costs.

¹ *Freedom of Information in New Zealand*, 1992.

² Law Commission, *Review of the Official Information Act 1982*, October 1997.

³ Fifty submissions were received on the discussion paper from a wide variety of individuals and agencies.

SECTION BY SECTION DISCUSSION

5.2 SECTION 33 - Application

- 5.2.1 Section 33 provides that Part V of the Act applies to what is termed an “information privacy request”. An information privacy request is:
- a principle 6(1)(a) request to confirm whether an agency holds personal information;
 - a principle 6(1)(b) request to be given access to personal information;
 - a principle 7(1) request to correct personal information.
- 5.2.2 “Information privacy request” is a handy shorthand for these access and correction requests and it is a defined term in section 2. One submission suggested that a better title for these requests could be devised and proposed that they be called “personal information requests”. It is true that “information privacy request” has no ordinary meaning and is only understandable by its definition in section 33. However, that may even be an advantage compared with the plainer phrase “personal information request” since it encourages people to seek the statutory definition. On balance I do not recommend any change.

5.3 SECTION 34 - Who may make requests

- 5.3.1 Information privacy requests may be made by New Zealand citizens and permanent residents (wherever they are) and by any other individual who is *in* New Zealand.
- 5.3.2 An Australian, for instance, who may formerly have lived and worked for many years in New Zealand, has no right of access to information still held about him or her unless an information privacy request is made during a visit here. If a New Zealand agency does hold information about an individual who is neither a citizen or a permanent resident, that individual’s right of access to information should not depend on whether or not they happen to be in New Zealand at the time. After all, the fact that people are neither citizens or residents of New Zealand nor present in the country does not bar them from making a complaint if they believe that a New Zealand agency has dealt wrongly with their personal information.⁴
- 5.3.3 I recommend below that the law be changed so that the denial of the right of access to non-New Zealanders who are not present in New Zealand at the time should be done away with. Most submissions on the discussion paper agreed that the present standing requirement should be dropped.⁵ Before discussing some of the practical issues arising from the recommendation, I outline some of the considerations that have convinced me of the desirability of the change.

Importance of access and correction rights

- 5.3.4 Access and correction rights count amongst the most important and fundamental in any data protection or information privacy law. The right to obtain access to information is an essential feature in ensuring that individuals can retain some control of their privacy and the information processed about them. Denial of the right of access means that individuals would, in many circumstances, be unable to know what information is being held about them and possibly used to their detriment. The right of access allows “light to be shined in dark places” to enable the individual to find out what is known, or believed, about him or her. By obtaining access to information the individual is also in a position to ensure that other information privacy principles are adhered to.

⁴ See section 67 permits complaints by “any person”.

⁵ See submissions L4, L5, L7, L9, L12, L14, L17, L19, L23, S2, S36, S37 and S45. Submissions L10 and L22 opposed the change.

- 5.3.5 If personal information is in error, an individual may normally request correction. Foreigners are doubly penalised by section 34 since it not only denies them the right to access information to see if it is correct but also denies the right to seek correction or ask that a correction statement be placed with the information. This is simply not fair and does not accord with the spirit of an information privacy law. Nearly all submissions supported allowing people overseas having access to information held in New Zealand.⁶
- 5.3.6 Removing the bar on the right of access and correction will put right something that is clearly wrong in the Act. If New Zealand agencies are in the position of holding personal information about foreigners it is incumbent on them that they comply with the information privacy principles in respect of that information. The Act generally makes no distinction between New Zealanders and others. However, to deny the right of access and the right to correction removes one of the most important mechanisms for ensuring that the principles are indeed complied with.

International considerations

- 5.3.7 I can see no justification for the present denial of the rights to foreigners in relevant international instruments. Most particularly, the OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data provide no basis for such a distinction being made. I am not aware that the lack of foundation existing in the OECD Guidelines for the distinction made in section 34 was considered at the time the Privacy of Information Bill was being considered. Rather, the approach had been to simply carry over the procedural provisions for giving access and correction that had been in the Official Information Act. Now is an appropriate time to reconsider that matter.
- 5.3.8 Of particular concern at this time is the fact that our Privacy Act will be subject to scrutiny by the European Union as to whether it provides “adequate” protection for personal data about Europeans transmitted to New Zealand for processing.⁷ I believe that the Act offers adequate protection in virtually all respects. In some aspects its standards exceed those in Europe. However, I fear that the EU will see the non-availability of legal access and correction rights to Europeans while in Europe as a feature that is not “adequate” in terms of the Directive. This provides an incentive to change the present provisions since it would be unfortunate to have our otherwise excellent and “adequate” privacy law called into question on this one small feature.
- 5.3.9 At a general human rights level the United Nations International Covenant on Civil and Political Right provides that no-one may be subjected to arbitrary or unlawful interference with his privacy (article 17) and that everyone has the right to receive and impart information (article 19). States are to recognise and ensure the rights recognised in the Covenant without distinction of any kind including, amongst others, those based on national origin (article 2).
- 5.3.10 At a more specific information privacy level the United Nations General Assembly has adopted Guidelines for the Regulation of Computerised Personal Data Files.⁸ These guidelines are not well known since most countries with privacy laws tend either to look to the OECD Guidelines or to the Council of Europe or European Union instruments. Nonetheless, New Zealand usually takes cognisance of UN instruments notwithstanding that General Assembly resolutions are not binding.⁹

⁶ Of the 17 submissions on this issue, 14 supported change, 2 opposed or were not aware of a need for change, and 1 did not answer the question asked.

⁷ EU Directive on Data Protection, article 25.

⁸ These 1990 guidelines have been republished in *Privacy Law and Practice*.

⁹ Under section 14(c) of the Act I am directed to take account of international obligations accepted by New Zealand.

- 5.3.11 Clause 4 of the UN guidelines sets out a “principle of interested party access” which essentially refers to the right of access found in information privacy principle 6. The clause states:

“It is desirable that the provisions of this principle should apply to everyone, irrespective of nationality or place of residence.”

Legislative history

- 5.3.12 Section 34 has been carried over from section 24(2) of the Official Information Act 1982. The limitation in section 24(2) of the Official Information Act was not included as a recommendation of the Committee on Official Information and therefore the Danks report offers no explanation for it.¹⁰ Standing requirements were introduced at the select committee stage of the Official Information Bill.¹¹
- 5.3.13 It has been suggested by some commentators that some of the standing requirements existing in the Official Information Act seem rather pointless given that they can sometimes be circumvented through the appointment of New Zealand agents who can seek official information in their own right.¹² However, it is not possible to bypass the standing requirements through requests for personal information and, of course, in the Privacy Act context private sector agencies will not be subject to the Official Information Act.
- 5.3.14 It has been noted elsewhere in this report that existing statutes were heavily drawn upon as models in the drafting of the Privacy of Information Bill. Prime amongst these were the Official Information Act and the Ombudsmen Act. However, another model was the Privacy Act 1988 (Commonwealth of Australia). That statute has no direct equivalent of section 34 although section 41(4) provides that the Privacy Commissioner shall not investigate a complaint alleging a breach of information privacy principle 7 (which like in the New Zealand Act, concerns correction of personal information) unless the individual concerned is:
- an Australian citizen; or
 - a person whose continued presence in Australia is not subject to a limitation as to time imposed by law.
- 5.3.15 The Australian Privacy Act has no such restriction in respect of access complaints. However, it only covers the Commonwealth public sector and the practice there is for access complaints to be normally taken to the Australian Administrative Tribunal under the Freedom of Information Act in any case.¹³ I cannot see that the Australian model commends itself since foreigners should also be able to seek correction of inaccurate information as well.
- 5.3.16 The Wanganui Computer Centre Act 1976 is relevant to the legislative history of the Privacy Act. This contained no standing requirement of the type found in section 34. Accordingly, one of the unintended consequences of repeal of the 1976 Act is that foreigners who may have lived a portion of their lives in New Zealand but left the country will have lost their entitlement to seek criminal history information that they could have obtained under the 1976 Act. This might include, for example, details of convictions or confirmation that during that period they had no such convictions. I am confident that it was not the intention that the Privacy Act so limit pre-existing entitlements. In-

¹⁰ See Committee on Official Information, *Towards Open Government: Supplementary Report*, 1981, page 78.

¹¹ See (1982) 449 NZPD 5052.

¹² See *Freedom of Information in New Zealand*, pages 70-72.

¹³ The Australian Act covers the private sector in relation to credit reporting. There appears to be no limit on individuals seeking access to, or correction of, credit reports based upon citizenship, residence, or presence in Australia.

deed, the repeal of the 1976 Act was done in the belief that the Privacy Act would provide continuing rights and entitlements of an enhanced character. In the case of foreigners whose information is held in New Zealand this has proved not to be the case.



RECOMMENDATION 61

The standing requirements in section 34 should be abolished.

Practicalities concerning overseas requests

- 5.3.17 I considered whether the regime should give access rights based upon the existence of reciprocal rights for New Zealanders but have concluded that this would be impractical and has little to commend it. Such an approach would, for example, mean that a request from a person in Europe would have to be actioned but not one from a Pacific Island country. The position would become complicated with respect to a jurisdiction such as Australia where New Zealanders may request copies of their credit reports but otherwise have no access rights to personal information held by private sector organisations. Furthermore, any such distinction would likely *increase* rather than *decrease* compliance costs. The average agency would not be in any position to judge whether New Zealanders had access rights in another jurisdiction and it might involve more work in trying to establish this than in responding to an occasional request.
- 5.3.18 A number of submissions suggested that agencies should be permitted to make a reasonable charge for the costs of giving such access. Two submissions suggested that it should be possible to insist that the overseas requester provide a New Zealand-based agent and address to which the information could be directed.¹⁴
- 5.3.19 I do not see any merit in the latter suggestion. This would impose costs upon requesters which may be, in some cases, prohibitive. Although there may be some particular circumstances where the appointment of an agent may be a reasonable requirement, for example if the only appropriate way to give access is by way of inspection of documents, for the most part an agent will be of little assistance. On the other hand, if a requester already has an agent present in New Zealand, the agent may be a convenient conduit to give access. An example might be where an individual is pursuing an immigration application and they have a New Zealand lawyer.
- 5.3.20 Private sector agencies can make a reasonable charge for giving access whereas public sector agencies may not. A case can be made that public sector agencies should in some circumstances be entitled to make a reasonable charge for giving access to individuals who are not in New Zealand and who are neither New Zealand citizens nor permanent residents, or for meeting the additional costs of such overseas requests.¹⁵ Although the costs for sending documents or information overseas should not be exaggerated (since this is an everyday occurrence for many businesses in the 1990s), the costs are likely to be greater than giving access to a person who is in the country. There may also be some additional costs in the precautions needed to verify identity or authorisation.
- 5.3.21 I suggest that the current regime allowing private sector agencies to make a reasonable charge, as set out in section 35, should provide the basis for any charging by public sector agencies in the relevant circumstances. This might be achieved by amending section 35 or 36. The first would be appropriate if public sector agencies are to be generally permitted to make such charges for overseas requests from foreigners, the latter if an agency needs to make out a special case. Alternatively the no-charging rule could be left in place to await to see if a problem develops.

¹⁴ Submissions L9 and S36.

¹⁵ Although this might be viewed as discriminatory on the basis of national origin or citizenship, I expect that such a distinction would be considered justifiable.

“The Insurance Council would have no objection to overseas based individuals making requests for their personal information, provided the fact that they were overseas would not add compliance costs to meeting the access request.

- INSURANCE COUNCIL,
SUBMISSION L9

**RECOMMENDATION 62**

Public sector agencies should be entitled to make a reasonable charge, of the type permitted by section 35, for making information available to an individual overseas who is neither a New Zealand citizen nor permanent resident.

Adoption (Intercountry) Act 1997

- 5.3.22 The Adoption (Intercountry) Act 1997 implements the Hague Convention on intercountry adoptions. Amongst other things, the Convention provides that States must ensure that children the subject of intercountry adoptions can obtain access to information about their origins.¹⁶ The select committee studying the bill concluded that there were extensive rights of access to information already existing in the Privacy Act and that it was unnecessary to create a special regime in the Adoption (Intercountry) Act. However, the select committee noted my concern that some New Zealand adoptees living overseas might not qualify under section 34 of the Privacy Act if they no longer hold New Zealand citizenship.¹⁷ The committee recommended that there be an exception to section 34 where persons adopted under the Convention make a request for information about that person's origin. This was implemented in section 13(3) of the Adoption (Intercountry) Act which states:

“A person who is adopted in accordance with the Convention may make an information privacy request under the Privacy Act 1993 for information concerning the person's origin, notwithstanding that the person may not be a New Zealand citizen or a permanent resident of New Zealand or an individual who is in New Zealand, and section 34 of that Act shall be read subject to this subsection.”

**RECOMMENDATION 63**

If the general standing requirement in section 34 is removed then section 13(3) of the Adoption (Intercountry) Act 1997 should be repealed.

Parents and children etc

- 5.3.23 The Privacy Act allows individuals or their agents to make information privacy requests.¹⁸ There is no explicit provision for parents to exercise the right of access on behalf of children simply because of their status as guardians. Some have questioned whether this is satisfactory.¹⁹ The questioning is usually by parents and not by young people themselves.
- 5.3.24 Where information is held by a public sector agency it is possible for a parent to request information about a child and to obtain the information as might any other requester under the Official Information Act. However, the parent does not “stand in the shoes” of the child. The request is simply considered under Part II of that Act. There are more grounds for refusing requests under Part II of the Official Information Act than would apply to an information privacy request by the individual concerned. Furthermore, an information privacy request to a public sector agency is free of charge unlike a Part II Official Information Act request.
- 5.3.25 There are provisions in other statutes which enable parents or guardians to obtain information about their children. Typically these are framed around the types of information that are relevant to the duties of parents or guardians in

¹⁶ Convention on Protection of Children and Co-operation in respect of Intercountry Adoption, article 30.

¹⁷ See Report of the Privacy Commissioner to the Minister of Justice in relation to the Adoption Amendment Bill (No 2), July 1996.

¹⁸ Privacy Act, sections 34 and 45.

¹⁹ Note that disclosures may nonetheless be permitted to be made to parents within the discretion of the agency and consistently with principle 11.

“We see no reason why even quite young children should not appoint an agent to make a request on their behalf. Nor is there anything in the Privacy Act to prevent a child or young person making a request in their own right. Of course very young children may not have the capacity. In such cases we favour an amendment to allow a parent, guardian or court-appointed custodian to make a request on behalf of the child.”

- COMMISSIONER FOR CHILDREN,
SUBMISSION L3

caring for their children. For example, parents have certain rights in relation to a child’s educational²⁰ and medical information.²¹ If there is a problem in relation to parents getting access to information about their children one remedy will be the enactment of a specific provision in the appropriate statute rather than creating a general access right under the Privacy Act which would carry significant risks of undermining privacy in some cases.

- 5.3.26 Two prime privacy risks exist in any proposal to allow parents to exercise the access rights of the individual children. The first is that it may undermine the autonomy of children, particularly older children who are quite able to exercise access in their own behalf or to appoint their parents as their agents. A parent might also seek access to information about a child unbeknownst to the child concerned and then withhold that information from the child.
- 5.3.27 The second is that parents may seek access to information in a way that undermines the privacy of their children. As children get older, more independent and develop their own personality, they do, of course, have secrets from their parents. Some are only transitory. Sometimes they confide in outside agencies. There would be circumstances where a parent exercises a right of access ostensibly on behalf of a child but in fact regardless of, or even contrary to, that child’s wishes or best interests. It is clear that the interests of a parent and child can diverge. Sometimes those interests are in conflict. It would be risky to create a regime where the parent could invariably exercise entitlements conferred on their offspring as individuals.
- 5.3.28 Some privacy laws have attempted to allow parents or guardians to exercise the access rights of their children but with safeguards which seek to ensure that the risks are minimised. Most laws which tackle this matter do not stop simply at parents and children and also deal with the position of other individuals who may not be in a position to exercise their access rights. The following illustrates how laws in Hong Kong, Australia and Canada have tackled the matter.
- 5.3.29 The Hong Kong privacy law provides that a data access request may be made by “an individual or a relevant person on behalf of an individual”.²² “Relevant person” in relation to an individual means:

- “(a) where the individual is a minor, a person who has parental responsibility for the minor;
- (b) where the individual is incapable of managing his own affairs, a person who has been appointed by a Court to manage those affairs;
- (c) in any other case, a person authorised in writing by the individual to make a data access request, a data correction request, or both such requests, on behalf of the individual.”²³

The provision does not explicitly address the risks earlier discussed. It appears that access rights of relevant persons coexist with the rights of the individuals on whose behalf they act.²⁴ Any protection from the risks mentioned would have to be found in an interpretation of the phrase “on behalf of” the individual. Commentators have suggested that “on behalf of” would justify, if not actually require, an agency to refuse access to a parent where the data had been

²⁰ See Education Act, section 77.

²¹ See Health Act 1956, section 22F. A parent or guardian is, for the purpose of this section, the representative of a child under 16. The provision is subject to rule 11(4) of the Health Information Privacy Code 1994.

²² Personal Data (Privacy) Ordinance 1995 (Hong Kong), section 18(1).

²³ Personal Data (Privacy) Ordinance 1995, (Hong Kong), section 2(1).

²⁴ Berthold and Wacks, *Data Privacy Law in Hong Kong*, 1997, page 162.

“An amendment might clarify the issues surrounding the provision of school reports, although any amendment would need to take account of the fact that a parent’s rights to information should not override an older student’s wishes.”

- MINISTRY OF

EDUCATION, SUBMISSION L11

collected from a child on the basis of confidentiality.²⁵ The same commentators criticise the provision as placing agencies in a difficult position to adjudicate on parent-child disputes without explicit statutory guidance.

5.3.30 The Health Records (Privacy and Access) Act 1997 of the Australian Capital Territory provides that:

“Where the consumer is under 18 years of age, the right of access is exercisable:

- (a) if the consumer does not have the status under this Act of a young person - by the consumer personally; or
- (b) in any other case - on behalf of the consumer by a guardian of the consumer.”²⁶

The ACT law defines “young person” to mean:

“A person under 18 years of age, other than a person who is of sufficient age, and of sufficient mental and emotional maturity, to:

- (a) understand the nature of a health service; and
- (b) give consent to a health service.”²⁷

It goes on to provide that:

“Where the consumer is a legally incompetent person, the right of access is exercisable on behalf of the consumer by a guardian of the consumer.”²⁸

5.3.31 The ACT Act, unlike the Hong Kong Ordinance, addresses the question of autonomy of young people and precludes concurrent access rights between parent and child when a young person is fully able to exercise his or her own rights.

5.3.32 A similar approach is taken in certain Canadian provincial legislation. Typically such provisions would deal not only with requests by young people, but also those who are incapacitated and the persons who may request information in respect of deceased persons.²⁹ Many such provisions still fail to address all the risks mentioned although the Alberta legislation attempts to by stating that any right or power conferred on an individual by the Act may be exercised:

“If the individual is a minor, by a guardian of the minor in circumstance where, in the opinion of the head of the public body concerned, the exercise of the right or power by the guardian would not constitute an unreasonable invasion of the personal privacy of the minor.”³⁰

5.3.33 If provision were to be made it should have at least the following features in my view:

- an explicit indication that the right of access is to be exercised “on behalf of” the young person - the intention is not to give parents and others access to personal information for their own purposes;
- young people who are capable of doing so ought themselves to be able to exercise rights of access without having to await the age of majority;

²⁵ *Ibid*, page 163.

²⁶ Health Records (Privacy and Access) Act 1997 (ACT), section 10(6).

²⁷ Health Records (Privacy and Access) Act 1997 (ACT), section 4.

²⁸ Health Records (Privacy and Access) Act 1997 (ACT), section 10(7).

²⁹ See, for example, Freedom of Information and Protection of Privacy Regulations 1993 (British Columbia), clause 3 and Freedom of Information and Protection of Privacy Act 1994 (Alberta), section 79.

³⁰ Freedom of Information and Protection of Privacy Act 1994 (Alberta), section 79(1)(d).

- concurrent rights of access should not exist for both parents and child where the child is able to exercise rights on his or her own behalf;
- an agency should be able to refuse a request notwithstanding that a person has established status as a parent where it believes it is necessary to protect the privacy of the young person.

It would probably need also to address the issue of incapacitated persons. There may also be a case to limit the scope to certain types of information. For example, it might be inappropriate for a parent to be entitled to have access to information held by an employer about a 17 year old.

- 5.3.34 It would be difficult to develop such a provision. Given the lack of evidence of a problem with parents getting access to the information they need, I do not recommend its inclusion in the Act at this time. I am particularly mindful that the Commissioner for Children’s office did not support such a provision.³¹ There are obviously legitimate needs for parents to have access to information and it is desirable that there be mechanisms for this to occur. In the public sector these already exist in the official information statutes. The existence of a significant problem in the private sector is not apparent. In respect of both educational information and health information there are also already special additional access regimes in place.

5.4 SECTION 35 - Charges

- 5.4.1 Following the earlier regime under the Official Information Act 1982, public sector agencies may not make any charge for dealing with an information privacy request. However, private sector agencies are allowed to make a reasonable charge. The intention was that an ability to charge would minimise the cost to private sector agencies of meeting requests yet ensure that the restrictions upon charging would prevent the cost from becoming an appreciable barrier to individuals who wished to exercise their access rights. The Privacy Commissioner has the power to determine upon investigation in individual cases what is a reasonable charge. There have been relatively few complaints about charges. Due to the paucity of complaints I have so far issued only one case note.³²

- 5.4.2 While the basic position is quite simply expressed - the public sector cannot charge for an information privacy request whereas the private sector may, so long as the charge is reasonable - the section is, in fact, long and complicated. It has been necessary for the section to be quite precise about what can and cannot be charged for.

- 5.4.3 Although I consider that section 35 is largely adequate in substance it is unduly complex in its drafting. It may become further complicated by the proposal to entitle public sector agencies to make a reasonable charge for making information available to an individual overseas who is neither a New Zealand citizen nor permanent resident.³³ I therefore suggest that the opportunity be taken, if possible, to re-enact the entire section in a simplified way.³⁴



RECOMMENDATION 64

Section 35 should be redrafted in a simpler fashion.

Charging for correction

- 5.4.4 A submission was made that no charge should be permitted for correcting information in response to a principle 7 request.³⁵ The present position is that a public sector agency cannot charge for making a correction whereas a private

³¹ See submissions L3.

³² Case note 7844 involved a \$336 charge which was reduced to \$122.65.

³³ See recommendation 62.

³⁴ Use of the proposed new definition of “private sector agency” will assist in simplification. See recommendation 14.

³⁵ See submission K11.

“Any system of charging is likely to be challenged by those who see ability to pay as imposing an unreasonable constraint on a democratic entitlement. But a ‘free’ system of access would be a blank cheque for the use of public resources.”

- DANKS COMMITTEE
REPORT, 1991

sector agency may make a “reasonable charge”. Critics of the ability to charge see it as objectionable that an agency which accepts that information it holds ought to be corrected should be able to charge the individual for the privilege of doing so. Rather, they would say, the agency should be obliged to put the matter right at its own expense. I agree. Indeed, agencies would have a difficult task insisting upon payment for correction in cases of information conceded to be inaccurate since they are bound to address the issue, irrespective of the information privacy request, pursuant to principle 7(2). This precise point was put by the Rt. Hon. David Lange on the second reading of the Privacy of Information Bill when he stated:

“It seems slightly odd that a charge is made for correction of information. It seems to me that, if an agency holds incorrect information, it would be a matter of useful public service and perhaps a payment should be made to the person who drew attention to the inaccuracy of the information. ... It seems to me that there is another principle of privacy that is set out in the legislation: as soon as an agency knows that there is incorrect information, it is a matter of law in terms of the bill that it has to correct it. Therefore I suggest to the Minister that it is a total waste of time to put in a provision for charging someone to correct information, because the agency must, when it knows that the information is incorrect, change it. All that a person needs to do is not to make a complaint, but just to draw the agency’s attention to the fact that the information is wrong - require it to do nothing except follow the law. There can be no possibility of that person’s receiving a charge. It is incumbent on the agency to correct it.”³⁶

- 5.4.5 Indeed, the absurdity can be taken one step further. If the individual concerned requests a private sector agency to make a correction a charge may be made. If the individual asks a friend to request the agency to make the correction no charge may be made. However, if the correction is not made the individual concerned may still lay a complaint that the agency has breached principle 7(2) in the circumstances.
- 5.4.6 Accordingly, I recommend that section 35(3)(b)(i) be repealed so that no charge may be made for the correction of information in response to an information privacy request. I do not expect this to cause any difficulty for agencies since a charge is hardly ever made. However, I suggest that section 35(3)(b)(ii) be left in place so as to allow a reasonable charge to be made, in appropriate circumstances, for the attachment of a correction statement, which often arises where the agency does not accept that the information is incorrect - and therefore differs from correction itself.³⁷ The attachment of the statement is sometimes seen as a way of resolving a complaint whether there are irreconcilable views on the accuracy of the information. However, there are rare cases where a requester might place unreasonable burdens on an agency if a charge could not be made. I have in mind the case of persons who may present excessively long statements or who repeatedly submit correction statements to “update” information on file.



RECOMMENDATION 65
Section 35(3)(b)(i) should be repealed.

³⁶ NZPD, 20 April 1993, page 14726.

³⁷ Sometimes the correction statement process is used where it *is* conceded that information is incorrect but it is not feasible, or is undesirable, to change the information held itself.

“Public sector agencies should have the option to charge. Public sector agencies work in competitive, cost recovery environments and not being able to charge conflicts with these requirements.”

- WELLINGTON CITY COUNCIL,
 SUBMISSION G12

Misuse of access right

- 5.4.7 One rationale for the right of private sector agencies to impose reasonable charges for making information available was expressed by Hamish Hancock, the Chair of the Justice and Law Reform Subcommittee studying the Privacy of Information Bill, as follows:

“Agencies, businesses, and private organisations need to be protected against people who make excessive or vexatious demands on them. Having the power to charge for giving access to information is a protection that I believe those organisations will welcome.”³⁸

- 5.4.8 The relatively few complaints about charging probably indicates that the regime is working reasonably well. In some other jurisdictions, particularly those which provide for standard charges but allow requesters to seek a waiver, there has been a high volume of charging complaints (with attendant delay in granting access until the matter is resolved). My impression (not contradicted by evidence in submissions) has been that individuals have generally been responsible in their requests and that private sector agencies have been equally responsible in the levying of charges for making information available. Had this not been the case I would have expected to receive more complaints involving refusals based upon “frivolous, vexatious or trivial” grounds (section 29(1)(j)) or concerning excessive charges (section 35). This has not happened.

- 5.4.9 It has sometimes been suggested that requesters can “misuse” the right of access by submitting numerous or repeated requests for little purpose except perhaps to fulfil an obsession or to cause an agency inconvenience. There is little evidence of this being a problem in New Zealand in relation to the personal information access right.³⁹ In the public sector personal access rights have existed for between 10 and 15 years and little problem has been detected. In the private sector the ability to make a reasonable charge for the making available of the information would generally discourage most such misuse. In both the public and private sectors agencies may also refuse a request if it is frivolous or vexatious or the information requested is trivial.⁴⁰ The submissions did not disclose any significant problem of misuse of the access rights although the NZ Employers Federation suggested in a covering letter to submission L12 that:

“A matter of concern is the ability for the Privacy Act to be used as a tactical industrial weapon. Employees, have at times, put in myriad requests for personal information, for no better reason than a desire to cause disruption. This is an abuse of the Act of which the Commissioner needs to be aware.”

- 5.4.10 Although not common, such things may happen on occasion. Certainly, such incidents have not manifested themselves in any large number of complaints to my office (which might have been expected if an employer’s response was to impose a charge or to refuse a request as “vexatious”). I suspect that such access is simply granted or the issue is forgotten as the industrial dispute is resolved. Such requests may not be motivated by desire to be vexatious but in order to obtain information relevant to the industrial dispute - albeit at an inconvenient time for the employer. It should be added that trade unions and employee

³⁸ (1993) 71 NZPD 1413.

³⁹ It is more likely that such “misuse” may occasionally arise with Official Information Act requests which need not focus upon information about the individual concerned and which can be duplicated and sent to multiple agencies at the same time. Ontario, for example, has on occasion been plagued by requesters abusing the process with, for example, one person filing 1131 appeals simply to “have fun” at the expense of government agencies. See Information and Privacy Commissioner/Ontario, *Annual Report 1995*, page 12 and *Annual Report 1996*, page 12.

⁴⁰ See section 29(1)(j).

“The ability of the private sector to charge for access and correction of information should be withdrawn. It is unreasonable that the individual should be liable for costs of access to and correction of information in the employment context when they have no choice but to provide such information in the first place. We have had examples where cost has been a significant disincentive to employees accessing information held about them.”

- FINANCE SECTOR UNION,
SUBMISSION WX1

representatives also allege that employers sometimes fail to live up to their obligations to process access requests (especially when access is being sought urgently in the prospect of bringing a personal grievance).

- 5.4.11 The important thing is that there is no empirical evidence to support any claim of significant misuse of the right of access. Although there are some isolated incidents of complainants who have pursued more than one complaint against an agency, or several agencies, through my office and in one case to the Tribunal,⁴¹ I do not have evidence of a real problem. However, if there were a problem it would become acute at the agency, not review, level and I may not have heard of it. While it was not substantiated in submissions I do not discount the possibility of a small problem existing or developing in the future.
- 5.4.12 I canvassed in the discussion paper the possibility of adopting an approach taken overseas. In at least two Canadian provinces agencies can apply to a Commissioner for an exemption entitling them to disregard a particular access request, or a series of requests, received from a particular individual. For example, section 53 of the Freedom of Information and Protection of Privacy Act of Alberta states:
- “Power to authorise a public body to disregard requests
If the head of a public body asks, the Commissioner may authorise the public body to disregard requests under section 7(1) that, because of their repetitious or systematic nature, would unreasonably interfere with the operations of the public body or amount to an abuse of the right of access.”⁴²
- 5.4.13 The quoted provision allows a Commissioner to consider the pragmatic effects of such a pattern of requests and their genuineness. The provision is directed towards some of the same concerns that the frivolous, vexatious or trivial, grounds for withholding in section 29(1)(j) of the Act are directed - but on a general rather than case by case basis. The power also has some similarities to the law concerning vexatious litigants. When declaring a litigant vexatious, a court may require the person to obtain leave before issuing any further proceedings. The British Columbia Commissioner under a similar power has, in several cases, authorised agencies to disregard all requests from named respondents for a period of one year. In one case he obliged the agency to deal with only one request for a further year.
- 5.4.14 An exemption power of this type, if adopted, would be directed towards the very few individuals who misuse an access right to the complete exasperation of the agencies involved. Often the work involved with processing such requests is out of all proportion to their importance. Frequently the resource directed to the few is expended to the detriment of many genuine requesters awaiting access to information.
- 5.4.15 There was support amongst people making submissions for a provision like that existing in Alberta and British Columbia. Of the 13 submissions which addressed this issue, 9 were in support.⁴³ Four submissions opposed the proposal each taking the view that section 29(1)(j), allowing for refusal of requests, was adequate for the purpose of addressing any problems.⁴⁴
- 5.4.16 I believe that the provision has merit and could work effectively in New Zealand in the tiny number of cases where there is an abuse of the right of access.

⁴¹ In the case of *Mayes v Owairaka (No. 2)*, CRT decision 25/96, 21 October 1997, an award of \$500 costs was made against the *successful* plaintiff as the case had “imposed a burden on those connected with the school staff and the Board disproportionate to the outcome.”

⁴² Note that the Alberta law combines features of both our Privacy Act and Official Information Act - but solely with public sector coverage. Therefore the power is relevant to third party requests as well as personal access requests.

⁴³ See submissions N2, N4, N7, N8, N10, N11, N12, S36 and S52.

⁴⁴ See submissions N3, N9, N15 and S42.

Consideration would have to be given to whether the function should be conferred on the Commissioner or the Tribunal. A variant on the proposal would be to enable a public sector agency, on such an application, to make a reasonable charge for giving such access notwithstanding section 35.⁴⁵



RECOMMENDATION 66

The Commissioner or the Tribunal should be empowered to exempt an agency from having to deal with a particular individual’s access request for a fixed period where it can be shown that the individual has lodged requests of a repetitious or systematic nature which would unreasonably interfere with the operations of the agency and amount to an abuse of the right of access.

Charging guidelines

5.4.17 There is an express link between sections 35 and 46(4)(b) of the Act. That latter provision provides that a code of practice may:

“In relation to charging under section 35 of this Act:

- (i) set guidelines to be followed by agencies in determining charges;
- (ii) prescribe circumstances in which no charge may be imposed.”

5.4.18 So far I have not issued a code of practice which sets guidelines to be followed by agencies in determining charges. However, in the Health Information Privacy Code 1994 I utilised the power to prescribe the circumstances in which no charge may be imposed.⁴⁶

5.4.19 There is also a link between section 35 and the provisions dealing with complaints, most notably section 78. That provision, discussed at paragraph 8.16, provides that in respect of complaints concerning the reasonableness of charges, a determination by the Commissioner is “final and binding”. These are the only types of complaints for which the Commissioner can actually issue a binding determination. In other complaints where an investigation is complete, and settlement has not been achieved, the Commissioner merely issues an opinion which may be persuasive but not binding. Complaints can thereafter be taken to the Complaints Review Tribunal (other than charging complaints).

5.4.20 In the discussion paper I canvassed the possibility of creating a special guideline power in respect of charging. This would involve transposing the existing power to issue codes of practice on the subject into a separate type of binding instrument. To date codes of practice have not appeared to be a suitable vehicle for charging complaints since they have been issued to apply only to a sector or agency, whereas charging guidelines would likely need to apply across the board. Guidelines might offer a mechanism for providing greater certainty to requesters and agencies alike.

5.4.21 The proposal for charging guidelines received a mixed response from people making submissions.⁴⁷ Those opposed to the idea anticipated that such guidelines might be overly restrictive or prescriptive and that it might be difficult to anticipate the full range of individual circumstances. In my view, many such criticisms could be met by appropriately written guidelines.⁴⁸ Some saw it as an

⁴⁵ If this variant finds favour the resulting provision might appropriately be included in section 36.

⁴⁶ Clause 6 of that code circumscribes the ability of private sector health agencies to make a charge in respect of an information privacy request.

⁴⁷ Thirteen submissions supported the notion of guidelines (L2, L4, L7, L14, L19, S2, S11, S25, G17, S6, S21 S36 and S46). Six were opposed (L9, L10, L12, L23 and G19). Three took no position but were generally sceptical.

⁴⁸ Guidelines could specify that if a charge were to be made within a specified formula it would be considered in all cases to be “reasonable”. The guidelines could be written in such a way that the reasonableness of charges exceeding or outside the formula would have to be shown in the event of a complaint thereby avoiding a complete or inflexible restriction.

“The Association supports the suggestion that the Commissioner be empowered to issue guidelines on charging for access to information. Any guidelines should, however, ensure consistency with the recovery permitted by state agencies (for example under the Official Information Act) and ensure that a fair and reasonable charge for time and copying costs may be levied.”

- NZ BANKERS’

ASSOCIATION, SUBMISSION S25

inappropriate role for the Commissioner to issue charging guidelines. However, this ignores the fact that the Commissioner already has an ability to deal with charging by code of practice.

- 5.4.22 I have not been in a hurry to issue charging guidelines under the existing power I have in respect of codes of practice. I anticipated that it would be preferable to handle a number of complaints to build up expertise in the issues before developing any such guidelines. I have been surprised by the fact that charging complaints are so infrequent. The question for guidelines was raised for discussion in anticipation that agencies may wish to have greater guidance on the subject. However, in light of the consultation on this matter I do not recommend the creation of any further statutory guideline making power on the subject for the time being. I will keep the matter under consideration and, if appropriate, issue a code dealing with the matter or offer non-binding guidelines.

5.5 SECTION 36 - Commissioner may authorise public sector agency to charge

- 5.5.1 Although public sector agencies cannot generally make any charge for dealing with an information privacy request, the Privacy Commissioner has the power to authorise a particular agency to make such a charge where the agency satisfies the Commissioner that it is being commercially disadvantaged, in comparison with any competitor in the private sector, by the prohibition upon charging. No such application has yet been made.
- 5.5.2 In some ways section 36 may be seen as a potential inroad into the “no charging” regime in the public sector for personal access requests that had existed since 1983. It had no equivalent in the Official Information Act 1982. However, it is tightly circumscribed and experience to date suggests that the generally free availability of such information is not under threat.
- 5.5.3 I have earlier recommended that the standing requirement in section 34 be removed so that agencies must respond to information privacy requests from foreigners who are not in New Zealand at the time of the request.⁴⁹ It seems appropriate to permit agencies to recover their reasonable costs in handling such requests. One way of achieving this might be by amending section 36 which would avoid generally undermining the public sector no-charging rule.

5.6 SECTION 37 - Urgency

- 5.6.1 Section 37 requires an individual seeking urgent attention to an information privacy request to provide the agency concerned with the reasons for the urgency. The provision is based upon section 12(3) of the Official Information Act 1982. However, neither Act spells out what is to happen where a request has been identified as urgent. Neither Act imposes more restricted time limits nor indicates that any consequences will be visited upon an agency where the regular time limits are missed even for an urgent request.
- 5.6.2 Failure to spell out the consequences of labelling a request “urgent” is probably less profound in respect of the Privacy Act than for requests under the Official Information Act. If an Official Information Act request is not considered in a timely fashion, the most that will likely happen on review is that access ultimately is required to be given. Under the Privacy Act regime this also will happen but the Complaints Review Tribunal might also award damages for any harm suffered through an “interference with the privacy of an individual”. It might therefore be possible for the individual requester in due course to receive

⁴⁹ See recommendation 61.

“Information held by public sector agencies should continue to be provided to an individual free of charge. Where however the information is to be used by a private sector organisation for clear commercial advantage then the organisation should be expected to pay a contribution to the public sector agency towards the cost of providing the information.”

- CLIVE COMRIE, SUBMISSION G1

both the information to which he or she was entitled together with damages for any harm suffered as the result of any undue delay in supplying it.⁵⁰ In cases of urgency it would presumably be more straightforward for an individual to show damage and more difficult for the agency concerned to show that it mitigated the damage given that it knew that the request was truly urgent.

- 5.6.3 There would be disadvantages in too precisely spelling out the consequences of identifying a request as urgent. For instance, it may be inappropriate to simply substitute a ten-working day limit in place of the 20-working day limit when the urgency of the case involving a request for a single document may justify same day action. If the regime for dealing with urgent requests was made too rigid it might encourage false claims of urgency to be placed on the “fast track”. On the other hand, it seems unsatisfactory for section 37 to set up a process for identifying urgent requests and then to remain silent on how those must be dealt with.
- 5.6.4 The matter was considered by the Law Commission in its review of the Official Information Act. The Commission’s report did not make any recommendations but did offer some observations based upon the Ombudsmen’s experience. It noted for example that the obligation upon agencies is to respond as soon as reasonably practicable even if this takes longer than requested - some requesters with urgent requests wrongly believe that they may impose a specific timeframe upon an agency to respond.⁵¹
- 5.6.5 The Law Commission also observed the Ombudsmen have issued guidelines on responding to urgent requests in the Official Information Act context. These emphasise that while each case must be assessed on its merits, relevant factors in determining what is reasonably practicable in the context of urgent requests include:
- the volume of information which must be considered;
 - the nature of the information requested and how it is held;
 - what consultations are necessary before making a decision on the request;
 - the specified reasons for urgency; and
 - whether according priority to an urgent request would unreasonably interfere with the agency’s operations.⁵²
- 5.6.6 While wishing to avoid precisely or rigidly spelling out the consequences of identifying a request as urgent, I consider that there may be merit in amending section 37 to make it clear that in cases where a request for urgency has been substantiated, an agency is expressly obliged to make reasonable endeavours to process the request with priority. On review, this would give scope also for considering whether “reasonable endeavours” were undertaken. An onus could be placed on agencies on review to show that information which was supplied after delay was indeed provided “as soon as reasonably practicable” - which is the existing obligation.
- 5.6.7 If change is to be made there may be merit in also considering the desirability of similarly changing the official information statutes.



RECOMMENDATION 67

Section 37 should be amended to make it clear that in cases where a request for urgency has been substantiated, an agency is obliged to make reasonable endeavours to process the request with priority.

- 5.6.8 According an urgent request priority would mean other requests in a queue take longer to be processed. In agencies which receive few requests this will not be a problem. However, in large government departments, or private sector

⁵⁰ See Privacy Act, section 66(4).

⁵¹ Law Commission *Review of the Official Information Act 1982, 1997*, paragraph 161.

⁵² *Ibid*, paragraph 162 and Office of the Ombudsmen, *Practice Guidelines No. 8*, April 1995.

“This question is raised in every seminar. Participants want to know what are the determining factors for considering a request urgent and how long should they take once a request is deemed urgent.”

- KATHRYN DALZIEL,

SUBMISSION S6

agencies having substantial personal information holdings, this can mean that requests that might otherwise be dealt with on a “first come first served” basis may take substantially longer to be completed where no case is established for urgency. However, two points occur to me:

- not all requests carry the same degree of priority as section 37 acknowledges - genuinely urgent requests appropriately should jump the queue and this will not necessarily seriously harm the interests of other requesters if the resultant delays are not excessive;
- agencies with large volume of requests do need to devote sufficient resources to handling the work satisfactorily and efficiently - agencies should allow some capacity to handle urgent requests.

Urgent cases on review

5.6.9 It will be apparent from elsewhere in this report that there is an excessively long queue in my own office for complaints. It might be thought that an individual needing access urgently to particular information will have “justice denied” if they come to my office and are faced with a 12 month queue to have the matter investigated. I consider that the under resourcing, and the resultant delays in having complaints investigated, is entirely unsatisfactory for *all* complainants - and indeed respondents - and not simply those who have an urgent information privacy request. However, my office does undertake a preliminary filtering of the complaints received and will bring cases substantiated as urgent to near the front of the queue. It is worrying that as the gap between available resources and volume of complaints widens there is the risk that my investigators could become almost fully engaged on urgent requests leading to even slower movement in the remainder of the queue.

5.6.10 There is the ability within the structure of the Act for an urgent request to be processed through an agency, and then my office, in a way that could then, if necessary, be taken to the Complaints Review Tribunal with great rapidity. This has not tended to happen as yet but the mechanisms do exist. In a recommendation affecting section 92 I seek a change which will better provide for urgent cases.⁵³ Furthermore, clause 7(2) of the Complaints Review Tribunal Regulations 1996 makes provision for rapid proceedings by allowing the Chairperson of the Tribunal to abridge the time for the filing of a statement of reply in access reviews where the “urgency” of the case so requires.

5.7 SECTION 38 - Assistance

5.7.1 Section 38 imposes a duty on agencies to render reasonable assistance to individuals in making their information privacy requests.

5.7.2 Virtually all information access laws contain such a provision since requesters will need a “helping hand” from time to time and the agency holding the information is in the best position to provide that. Indeed, the provision of assistance is frequently of mutual benefit since the agency also has an interest in a request being processed with the minimum of bother.

5.7.3 I have frequently observed, as have Ombudsmen, that if agencies took more care in discussing requests for information with requesters at the time of request, many requests which through misunderstandings are declined, could be satisfied. An agency which goes out of its way to provide assistance at the time that an individual is formulating, or has just made, a request will often reap the benefit through enabling requesters to more precisely define the scope of their requests. Frequently this can involve the limitation of a request to a particular fact or document thereby relieving the agency of a more burdensome search and collation concerning whole categories of information or documents.

⁵³ See recommendation 114.

Assistance and charging

- 5.7.4 It might be noted at this point that under section 35(4) a private sector agency may make a reasonable charge for the provision of assistance. Therefore, there is some scope for cost recovery for agencies outside the public sector. While some might fear that this lends itself to exploitation for the recovery of costs incurred in unwanted, expensive, excessive or over elaborate “assistance” this has not appeared to be the case as yet. Private sector agencies have shown a great deal of responsibility within the latitude afforded by the law and, of course, the provision for complaint if a charge is not reasonable provides an appropriate safeguard.

Assistance and urgency

- 5.7.5 Commentators on section 38, and the equivalent provision in the Official Information Act, have highlighted the link between the duty to provide assistance and the provision concerning urgency.⁵⁴ They have suggested that the duty to comply includes advising a requester who seeks information urgently that the requester needs to give reasons for urgent consideration but probably does not go as far as to require the agency to advise the requesters of their ability to seek the information urgently. While I do not recommend any change to the section at this stage to make the matter explicit, I would encourage agencies to be as helpful as they can in that regard and tell requesters of the need to ask for a request to be treated with urgency if the circumstances appear to warrant it.

5.8 SECTION 39 - Transfer of requests

- 5.8.1 Section 39 imposes a duty on agencies to transfer requests “promptly”, and in any case within ten working days, to another agency where the personal information requested is believed either to be held or to be more closely connected with its functions or activities.

Where individual does not want transfer

- 5.8.2 It may be desirable to amend the procedure established in section 39 so that an agency is relieved from the obligation to transfer a request in circumstances where it has good reason to believe that the individual does not wish the request to be transferred. The agency would, of course, have to inform the individual accordingly. This would address the privacy issue which occasionally arises whereby an individual deliberately chooses to ask one agency for information not wishing it to be known to a second agency that the request is being made. An example would be where the requester is an employee of an agency and fears that he or she might be labelled a “troublemaker” if known to be seeking out information about him or her which concerns the activities of his or her own employer.
- 5.8.3 I do not intend that where a request is received by agency X for information which is believed to be more closely connected with the functions or activities of agency Y (the ground for transfer in section 39(b)(ii)) that agency X be obliged to make information available in the circumstances where transfer is presently the appropriate course. Rather, in circumstances where, for example, the requester has said “I do not want agency Y to know of my request” I would like the section amended so that this very outcome is not required by law. Instead, I anticipate agency X explaining to the requester that really only agency Y can appropriately release the information and that normally the request would have been transferred but this has not been done so as to respect the requester’s wishes. The requester would be advised to ask agency Y directly for the information if he or she wishes to proceed.

⁵⁴ See *Freedom of Information in New Zealand*, pages 75-76, and *Privacy Law and Practice*, paragraph 1038.4.

**RECOMMENDATION 68**

Section 39 should be amended so that:

- (a) an agency is relieved of the obligation to transfer a request in circumstances where it has good reason to believe that the individual does not wish the request to be transferred; and
- (b) the agency duly informs the requester, together with information about the appropriate agency to which any future request should be directed.

5.8.4 A similar issue arises under the Official Information Act and consideration could be given, at some appropriate time, to the desirability of changing that Act.

5.9 SECTION 40 - Decisions on requests

5.9.1 Section 40 provides that the agency to which an information privacy request has been made, or transferred, must decide whether the request is to be granted and, if so, in what manner and for what charge. This decision is to be made as soon as reasonably practicable and in any case within twenty working days after the day on which the request was received.

What is the “time limit”?

5.9.2 There is a link between the time limits set out in section 40 and section 66 which defines “interference with privacy” for the purposes of complaints and remedies. In particular, section 66(3) provides that failure to comply with the “time limit fixed by section 40(1)” is deemed for the purposes of section 66(2)(a)(i) to be a refusal to make information available. If the Commissioner or Tribunal is of the opinion that there is no proper basis for a decision to refuse to make information available it will amount to an “interference with the privacy of an individual” for the purposes of Part VIII of the Act.

5.9.3 The phrase “time limit fixed by section 40(1)” might have one of several meanings:

- the full phrase included in section 40(1) “as soon as reasonably practicable, and in any case not later than 20 working days after the day on which the request is received by that agency”; or
- just the latter part of the phrase, that is “not later than 20 working days after the day on which the request is received by that agency.”

5.9.4 It seems to me that the primary obligation is to make information available “as soon as reasonably practicable”. The reference to 20 working days is to the outer limit. If the obligation is to make information available earlier, then it does not seem in keeping with the intention of the Act for the deemed refusal, and therefore remedies, to apply only from the time at which the outer limit is reached. In many circumstances the difference will not be critical and therefore the issue has not yet manifested itself in practical problems before me or the Tribunal. However, as a matter of principle it is important since the Act envisages access being given as soon as practicable and consistent delay until 20 working days is reached will undermine that statutory objective.

5.9.5 In certain urgent cases it may be critical for information to be made available by a particular date. If it is practicable for an agency to provide the information by that date, and it does not do so, then the failure to take the necessary decision might be important in respect of remedies. For example, if the delay can be characterised as a “deemed refusal” it will be possible to promptly lodge a complaint with my office even though the matter is still within the first 20 working days of the request having been lodged. In some cases, involving public sector agencies, the individual could also lodge urgent proceedings before the courts. After the event, it may be that the availability of damages will turn upon whether information made available within 20 working days had indeed

V

s 40

193

“We are surprised that there should be a time delay in providing access except where there is a charge. The practice in the public service has been to provide access/ information at the time of the decision, or thereafter at a time to suit the individual. The ‘decision’ has therefore been treated as meaning provision of the information/ access. It may be that if this is a problem with the Privacy Act there needs to be some amendment to the section to align the ‘decision’ and ‘access’.”

- STATE SERVICES COMMISSION,
SUBMISSION S11

been made available “as soon as practicable”. Although for most ordinary cases the difference will not be important it may be that in some instances, for reasons of urgency, the difference is critical in obtaining compensation for harm caused by the delay.

- 5.9.6 However, there are some arguments which might favour interpreting the phrase “time limit” as meaning 20 working days after the date upon which the request was received. Amongst these are:
- the phrase “time limit fixed” may connote a clearly fixed point which is difficult to ascribe to the point “as soon as reasonably practicable”;
 - the reference to “time limits” first appeared in the Official Information Act following a 1987 amendment which introduced the 20 working day reference;⁵⁵
 - the time limits provision should be utilised for failure to meet the clear outer limits for making a decision whereas section 66(4) (the “undue delay” provision) is more appropriately used for cases involving the making of a decision later than would have been “as soon as reasonably practicable”.⁵⁶ This appears to be supported by the authors of *Freedom of Information in New Zealand* where they state:

“The OIA originally imposed no time limits. Decisions had to be made ‘promptly’ or ‘as soon as reasonably practicable’. This language is still retained although the Act now imposes maximum time limits for decisions.”⁵⁷

- 5.9.7 It is necessary to clarify the issue. It is possible to simply await the Complaints Review Tribunal to make a decision on a relevant complaint to provide such guidance. This is an option to be considered. However, it may be a long time before a suitable test case comes forward. In the meantime, there is a degree of uncertainty for agencies in considering their obligations and risks under the provision and I will have to review many more cases in the interim simply on the basis of my interpretation. Many people will be fobbed off by an agency’s assertion that it has 20 working days to respond. The effect of the prevalent belief that agencies have 20 working days to respond, rather than being obliged to respond “as soon as practicable”, is detrimental to the operation of the Act.



RECOMMENDATION 69

Consideration should be given to clarifying the meaning of the phrase “time limit fixed” in section 66(3) so as to emphasise the primary obligation to give access “as soon as reasonably practicable”.

Subsections (3) and (4)

- 5.9.8 Subsections 40(3) and (4) were transferred from the Official Information Act 1982.⁵⁸ They require that a chief executive of a government department may either make the decisions on information privacy requests in person or delegate them to an authorised officer or employee, and that they may consult with anybody else about the decisions.
- 5.9.9 It was suggested in the discussion paper that these procedural provisions, being matters of the internal administration of such departments, may not be necessary or appropriate in the Act. Fifteen submissions were received in reply to a question asking whether section 40(3) and (4) could be repealed without affecting the operation of the Privacy Act. Fourteen answers replied that the

⁵⁵ Official Information Act 1982, section 28(4).

⁵⁶ This is not to suggest that section 66(4) is to be limited to such delays - the subsection is relevant to delays that occur *after* the taking of the decision.

⁵⁷ *Freedom of Information in New Zealand*, 1992, page 80.

⁵⁸ Official Information Act 1982, sections 15(4) and (5).

subsections could safely be repealed.⁵⁹ Of particular note, given that the subsections deal with administrative provisions concerning Government departments, both the Ministry of Justice and State Services Commission agreed that the subsections could be repealed.⁶⁰

5.9.10 A similar issue in relation to sections 15(4) and (5) of the Official Information Act was recently examined by the Law Commission.⁶¹ The Commission noted the origins of the Official Information Act provisions which had been included in 1987 amendments as a result of concerns expressed about that Act's operation in its early years. It also examined the provisions in practice and appeared to find them largely unnecessary in today's conditions. The Law Commission recommended that sections 15(4) of the Official Information Act should be repealed but that section 15(5) should be retained and perhaps broadened.

5.9.11 I note the Law Commission's recommendation to repeal section 15(4) of the Official Information Act and take the view that the equivalent section 40(3) of the Act should also be repealed. However, given the somewhat different considerations in the Privacy Act 1993 to the Official Information Act I do not see the need to retain, or broaden, section 40(4). I recommend its repeal also.



RECOMMENDATION 70

Section 40(3) and (4) should be repealed.

5.10 SECTION 41 - Extension of time limits

5.10.1 Section 41 provides for extending the time limits for making decisions on requests (section 39) or for transferring requests to another agency (section 40). Extension is permissible if:

- the request is for a large quantity of information or necessitates a search through a large quantity of information, and meeting the original time limit would unreasonably interfere with the operations of the agency; or
- consultations necessary to make a decision on the request are such that a proper response cannot reasonably be made within the original time limit.

5.10.2 The section provides that the extension of the time limit is made by the agency itself and is given effect to by giving or posting notice of the extension to the requester within twenty working days of receipt of the request. The notice is required to:

- specify the period of the extension;
- give the reasons for the extension;
- state that the requester has the right to complain to the Commissioner about the extension; and
- contain such other information as is necessary.

5.10.3 The provisions governing extension of time limits are modelled upon those in the Official Information Act. The Law Commission recently reviewed the provision for extension of time limits in that Act and noted that not all requests can be answered in the prescribed period. A power of extension is required for some large or difficult requests. It noted that the manner in which legislation expresses such a power presents several questions. The questions posed by the Law Commission would seem to have as much relevance in this context. The questions were:

- who should exercise the power in the first instance?
- on what grounds should it be exercisable?
- should the power be capable of being exercised more than once?

⁵⁹ See submissions L4, L5, L7, L9, L12, L13, L17, L19, L22, S11, S13, S18, S36 and S42.

⁶⁰ See submissions L22 and S11 respectively.

⁶¹ Law Commission, *Review of the Official Information Act 1982, 1997*, paragraphs 193-205.

- should there be an outer time limit on it?
- what provision should there be for review?⁶²

5.10.4 The Law Commission considered that the answers to the first and last questions should, in respect of the Official Information Act, be as at present. This also is my conclusion in respect of the personal access regime in the Privacy Act. That is to say, the agency which is handling the request should make the decision and give notice to the requester of the extension, the reasons for it, and the right to complain to the Privacy Commissioner: section 41. Complaints are handled by the Privacy Commissioner about extensions: section 66(2)(a)(v). I do not favour the approach provided for in some overseas access laws whereby an extension is granted or approved by a Commissioner.⁶³

Multiple extensions

5.10.5 The generally accepted interpretation of section 15A of the Official Information Act, and therefore presumably section 41 of the Act, is that the time for response can be extended only once - that action must be taken within 20 working days of receipt of the request. The Law Commission in its review agreed that the power should be limited in that way, and although it considered the possibility that something unforeseen might arise in the course of the extension requiring a further extension, it had no evidence of this being a problem in practice. The Law Commission did not propose any change to section 15A to allow multiple extensions of the time limit for responding to requests.⁶⁴ I know of no problem in respect of the Privacy Act suggesting a need for multiple extensions and also recommend no change.

Grounds for extension

5.10.6 The grounds for extension are the same in the Official Information Act and in the Privacy Act. The Law Commission considered whether there should be any further grounds. In particular it noted that there was a further ground in section 29A of the Official Information Act for the extension of time limits for compliance with requirements of the Ombudsmen. Section 93 of the Act corresponds to section 29A. It too has an additional ground permitting extension of a time limit for compliance with a requirement of the Privacy Commissioner, namely where:

“(c) The complexity of the issues raised by the requirement are such that the requirement cannot reasonably be complied with within the original time limit.”

5.10.7 The Law Commission recommended that the complexity of the issues raised by the request should be added to the grounds for an extension of time under section 15(1).⁶⁵ I agree that a similar recommendation should be made in respect of section 41.



RECOMMENDATION 71

Complexity of the issues raised by a request should be added to the grounds for an extension of time under section 41(1).

⁶² *Ibid*, paragraph 174

⁶³ See, for example, Freedom of Information and Protection of Privacy Act 1994 (Alberta), section 13(1) and Freedom of Information and Protection of Privacy Act 1992 (British Columbia), section 10(1), each of which provides for extension of time limits “with the Commissioner’s permission”. The British Columbia Information and Privacy Commissioner handled 107 requests by public bodies for time extensions in 1995/96 (source: Office of the Information & Privacy Commissioner of British Columbia, *Annual Report 1996/97*, page 55).

⁶⁴ Law Commission, *Review of the Official Information Act 1982, 1997*, paragraph 176.

⁶⁵ *Ibid*, paragraph 183.

Outer time limit

- 5.10.8 The Law Commission did not directly answer its question as to whether there should be an outer time limit placed upon extension. However, clearly the Commission was of the opinion that no such express limit was needed since no recommendation was made. I make no recommendation to place an express outer limit on the extension. At present, no problems have been uncovered justifying the need for such a change. Furthermore, the general obligations, and the provision for complaint, would seem to provide appropriate safeguards against excessive and unnecessary extensions.

“As soon as reasonably practicable”

- 5.10.9 In the discussion of section 40 I outlined the risks to access entitlements of an attitude that a response could be made within the outer limits prescribed by the Act rather than, as intended, “as soon as reasonably practicable”. In line with my recommendation in respect of section 40,⁶⁶ section 41 should also be revised. In particular, I suggest that the notice advising an individual of an extension of time limits should be given as soon as reasonably practicable not simply within the outer time limit.

**RECOMMENDATION 72**

Section 41(3) should be amended by replacing the phrase “within 20 working days” with “as soon as reasonably practicable, and in any case not later than 20 working days”.

5.11 SECTION 42 - Documents

- 5.11.1 Section 42 sets out the ways in which information contained in a document may be made available. Unless there are good reasons for providing the information in another form, the information is to be made available in the way preferred by the person requesting it. I have recommended elsewhere that the marginal note to this section be changed from “documents” to a more informative “making documents available”.⁶⁷
- 5.11.2 The term “document” is defined in section 2. I have recommended that consideration be given to adopting a new definition of “document” in section 2 in conjunction with any redefinition of the term in the proposed Evidence Code.⁶⁸

Origin and operation of provision

- 5.11.3 Section 42 is closely modelled upon section 16 of the Official Information Act 1982. There have been a number of opinions rendered upon the provision by the Ombudsmen and these have provided guidance to me in the exercise of my complaints function and by agencies in applying section 16. Furthermore, I have considered a number of complaints which have raised issues under section 42 and have reported on one of these in a case note.⁶⁹ In that case, the agency held voluminous files relating to the individual stretching back over twenty years. The agency had declined to provide a photocopy of the entire contents, as had been requested, but had instead invited the complainant to view his files and had offered to photocopy any parts that he wished to take away. I found this arrangement to have been reasonable in the circumstances.
- 5.11.4 The provision has also been the subject of judicial consideration in at least one case. The District Court considered whether or not making information available would impair efficient administration in *Police v Evans*.⁷⁰ In that case, the

⁶⁶ See recommendation 69.

⁶⁷ See recommendation 2.

⁶⁸ See recommendation 11.

⁶⁹ Case note 7602.

⁷⁰ [1996] DCR 65.

defendants applied, pursuant to their right to personal information under the Privacy Act, for tape copies of audio recordings that had been obtained by interception warrants. The defendants had been charged with a number of offences of receiving, breaking and entering, and conspiring to break and enter. The Police transcribed 508 evidential telephone conversations taken from 345 tapes, and this written transcription was proposed to be supplied to the defendants. Moreover, the Police were prepared to permit counsel, presumably with clients present if requested, to listen to the actual tapes at the police station. However, the defendants requested that copies of the personal information be made available in the form of actual audio recordings. The judge considered the issue, and other issues relating to access to the information, and held that the Police had satisfied the requirement of section 42(2)(a).

- 5.11.5 The provision on documents has as its origin a clause in the bill prepared by the Danks Committee.⁷¹ The Danks Report indicated that the clause had been based upon a provision in a 1978 Netherlands law. Given its age, the provision continues to work remarkably well.
- 5.11.6 In the last 20 years there have been remarkable changes in the form of documents and the methods for making them available; one need only consider the developments in photocopying, as a method of everyday reproduction, and faxes, as a method of transmission. Those are not in any sense “cutting edge” technologies. More recently we have the commonplace use and exchange of computer disks and CD-Roms, electronic transmission through private networks and the Internet, scanning of documents, optical character recognition software, voice recognition software - the list could go on.
- 5.11.7 Section 42 has stood the test of time through being expressed in relatively general terms. The phrase “providing the person with a copy of the document” may have begun its life with the notion of carbon copies and mimeographs in mind. However, it just as easily encompasses photocopying, the production of duplicate floppy disks or the printing of “hard copies” from a computer.
- 5.11.8 However, section 42 is not simply intended as a general statement of principle - the methods listed particularise the ways in which information in the form of a document may be made available. For this reason, while retaining the generality of aspects of section 42(1) I have considered whether there may be benefit in particularising some of the forms in which documentation might be made available. However, having studied the provision it is not apparent that it can be successfully improved in that respect. Change in that regard, if it were to occur, would have to appear in the definition of “document”. I have canvassed elsewhere whether that should be made more particular or more general to take account of new technology.⁷²

Loans of documents

- 5.11.9 It has been suggested that the provision should provide that an agency may make a document available by lending it to the individual for a reasonable period. This is already provided for in the Quebec public sector access law.⁷³ While section 16(1)(a) presently speaks of giving the person “a reasonable opportunity to inspect the document”, “inspection” unlike “loan” does not carry the connotation of a requester’s possession of the document for a period.

⁷¹ Committee on Official Information, *Towards Open Government: Supplementary Report*, 1981, pages 71-72. The provision appears to actually give stronger rights to the individual requesting access than had been contemplated in the Danks provision which only provided that the agency giving access would be “guided” by the preference of the person requesting the information.

⁷² See paragraphs 1.4.71 - 1.4.73.

⁷³ An Act respecting Access to Documents held by Public Bodies and the Protection of Personal Information (Quebec), section 13(3).

- 5.11.10 In many cases an agency may consider a loan of original documents as an unacceptable risk in terms of efficient administration.⁷⁴ The agency could refuse a requested loan under section 42(2)(a) for this reason. However, it should be remembered that the access contemplated is only by the individual concerned and in many cases the individual's and the agency's interests will coincide in having the document on loan protected and duly returned.
- 5.11.11 I do not see huge scope for the lending of documents in circumstances where access is currently being provided in other ways. Nonetheless, it may be argued that in the circumstances where a loan of documents will suitably meet the needs of both requester and agency the option should be expressly allowed for in the Act. In terms of compliance costs, there may be occasions where an agency will, under this proposal, be able to offer a loan of the original documentation and not have to meet copying costs. In such circumstances the individual may read the documents and, if a copy is to be made, bear his or her own costs. Notwithstanding such considerations I have decided not to recommend adoption of the idea as I fear that some requesters will seek to have a loan of documents in inappropriate circumstances and this alone would attract a measure of dispute and complaints.

5.12 SECTION 43 - Deletion of information from documents

- 5.12.1 Section 43 provides that where there is good reason for withholding some of the information contained in a document, the other information in that document may be made available by releasing a copy of the document with such deletions or alterations as are necessary.
- 5.12.2 The process of deletion of information from documents is one means by which the individual right of access is maximised while protecting competing interests. It provides a "middle way" between withholding a complete document, because something in that document may properly be withheld, or releasing that document, to the detriment of the interests protected by the various good reasons for withholding information.
- 5.12.3 When deleting material from documents it is often a simple matter to strike out certain passages. For practical reasons, the method that I recommend is to make a copy of the relevant page of the document, strike out the material to be withheld with a black marker pen, and then re-photocopy. Unless this final process of re-photocopying the page is undertaken it may be possible that the underlying material remains legible in certain conditions.
- 5.12.4 For agencies handling a high volume of requests there are also photocopying machines now available which can copy documents with portions enclosed by special marker pen which automatically mask the excised portions. The application of this technology overseas to the task has enabled the saving of time on an otherwise laborious manual task while leaving on file a clean copy of an entire document, with highlighted excised portions, easily amenable to review by a complaints body such as my office. I am aware of such machines being used in the law enforcement and social security contexts in Canada and the USA.
- 5.12.5 Section 43 was modelled on a provision in the Official Information Act which was itself recommended by the Danks Committee.⁷⁵ The provision has been

⁷⁴ If this ground was not seen as sufficient to refuse a loan in inappropriate circumstances, it could be provided, if the idea was adopted, that any loan is to be made in the sole discretion of the agency. The Act also implicitly allows the agency to place conditions on the loan - section 66(2)(a)(ii).

⁷⁵ See Official Information Act 1982, section 17, and Committee on Official Information, *Towards Open Government: Supplementary Report*, 1981, page 72.

the subject of a variety of opinions from the Ombudsmen which have been of assistance to me in my work. I also have rendered opinions which touch upon the deletion of information from documents and have occasionally included these in case notes. In one case note I described a complainant who wished to obtain access to information contained in two letters alleging that she had been involved with selling drugs at a school. In that case a typed copy of the letter was provided with certain material deleted. Typing was necessary since the handwriting might have identified the informant which was the information appropriately withheld in that case.⁷⁶

5.13 SECTION 44 - Reason for refusal to be given

- 5.13.1 Section 44 provides that where an agency refuses an information privacy request, it must give the requester:
- the reason for the refusal;
 - the grounds in support of that reason if the individual so requests; and
 - information concerning the right to complain to the Privacy Commissioner.
- 5.13.2 Section 44 is a critical provision. In drafting terms, it owes its immediate origin to section 19 of the Official Information Act. However, in terms of the international approach to information privacy it has as its origin the “individual participation principle” in the OECD Guidelines.⁷⁷

5.14 SECTION 45 - Precautions

- 5.14.1 Section 45 requires agencies to take appropriate precautions to ensure that personal information requested under principle 6(1)(b) is released only to the individual to whom it relates or to that individual’s duly authorised agent.
- 5.14.2 This provision is another one derived from the Official Information Act. It is unusual in that it is an area where there has been deviation, perhaps of some significance, from the recommendation of the Danks Committee. The clause recommended by Danks did not include any equivalent of section 45(b)(ii) which anticipates requests being made by an agent of the individual. Instead, the Danks clause would have required agencies to have adopted procedures to ensure that the information intended for an individual “is received only by that individual in person”.⁷⁸
- 5.14.3 The change to permit the making of access requests by agents is not simply a small drafting matter or consequent upon the Danks Committee failing to have considered an issue. Instead, the Danks Committee *expressly* made the following comments:

“This follows the concept of the Wanganui Computer Centre Act 1976 provisions ...

“To minimise the danger that the right of access will be misused by others no provision is made for information to be given to an agent, eg. a relative or a solicitor.”⁷⁹

- 5.14.4 It does not appear that widespread problems have been caused by agents misrepresenting or exceeding their authority in seeking access to information. However, I am aware of cases where persons who have obtained authorisation for information to be released to them to misrepresent themselves as an indi-

⁷⁶ Case note 2438.

⁷⁷ OECD Guidelines, clause 13(c).

⁷⁸ Committee on Official Information, *Towards Open Government: Supplementary Report*, 1981, page 79.

⁷⁹ *Ibid*, page 79.

vidual's agent.⁸⁰ I am also aware of a case where it was alleged that the agent, or authorised person, further misrepresented the position by photocopying an authorisation given for one purpose onto a fax to an agency making it appear that the individual had specifically authorised the access request. In such circumstances, the obligation on agencies to take precautions to ensure that information is only released to the individual or the individual's duly authorised agent become particularly important.

- 5.14.5 While there is naturally a desire by many agencies to be as helpful as possible, and to act upon remote requests, appropriate precautions must be taken to ensure that information only arrives in the correct hands. In the case of a faxed request, for example, it may be appropriate to commence work on assembling the requested information on the basis of such a request but to indicate to the requester that the original signed authorisation must be sighted before the information will be released. Similarly, telephone requests can sometimes be checked by taking the caller's telephone number and ringing back to a number held on file.

⁸⁰ The difference is that an agency is bound to deal with access request properly made by an agent in accordance with the requirement of the Act whereas disclosure, even to an authorised person, remains in terms of the Act a discretionary matter for an agency.

Part VI

VI

Codes of Practice and Exemptions from Information Privacy Principles

203

“We endorse the mechanism of privacy codes of practice. Although not widely used, its existence is extremely important in maintaining a credible, sustainable privacy regime.”

- NZ Law Society Privacy Working Group, submission N16

“The Health Information Privacy Code is a very accessible tool.”

- NZ College of Midwives, submission N9

“The provision of codes where specific needs arise is one of the more useful pieces of flexibility available to affected industries or activities under the Act. We note, however, the wide powers of the Privacy Commissioner in drafting, accepting and amending codes of practice. There are significant constitutional issues in giving unelected officials such as the Privacy Commissioner the right to put in place codes which are potentially more restrictive than the law itself.”

- Commonwealth Press Union, submission N13

“The lack of resources and resulting inability of the Commissioner’s Office to review and issue codes of practice in a timely manner negates the benefits of offering such a specialised mechanism within the Act.”

- NZ Law Society Privacy Working Group, submission N16

“If there are to be separate intelligence organisations, then in no respect should they be above or exempted from the laws of the land and in particular fundamental human rights laws such as the law protecting individual privacy. We favour the applicability of all of the privacy principles to intelligence organisations.”

- Auckland Council for Civil Liberties, submission O2

6.1 INTRODUCTION

Codes and exemptions

6.1.1 Part VI deals with codes of practice and specific exemptions. Twenty-one submissions were received on the discussion paper and a further 25 in response to a discussion paper on intelligence organisations.

6.1.2 Section 46 sets out what a code of practice is and what it may, and may not,

include. Section 53 explains the effect of a code, while sections 47 to 52 set out the processes for receiving, considering, and issuing, codes of practice. Sections 54 to 57 establish certain specific exemptions.

- 6.1.3 The following codes of practice have been issued:
- *Health Information Privacy Code 1993 (Temporary)* - section 52 allowed for the urgent issue of this temporary code, which has now expired;
 - *Health Information Privacy Code 1994* - the permanent replacement of that temporary code applying to the health and disabilities sector;
 - *GCS Information Privacy Code 1994* - which applied to a particular Government agency which was privatised, the code has now expired;
 - *Superannuation Schemes Unique Identifier Code 1995* - which modified principle 12 in the circumstances to which it applied;
 - *EDS Information Privacy Code 1997* - which replaced the GCS code;
 - *Justice Sector Unique Identifier Code 1998* - which modified principle 12 as it applied to certain justice sector agencies.

- 6.1.4 Very few specific exemptions have been granted under section 54 and generally between one and three have been granted each year.¹ In each case, the authorisation was granted to permit, in the public interest or for the benefit of the individuals concerned, a disclosure which would otherwise be a breach of principle 11.

- 6.1.5 The Act provides three other specific exemptions:
- section 55 excludes the application of the access and the correction principles from five classes of personal information;
 - section 56 provides an exemption relating to domestic affairs; and
 - section 57 exempts intelligence organisations from some of the principles.

Legislative history

- 6.1.6 The present provisions for codes of practice and exemptions differ significantly from what had been provided in the Privacy of Information Bill. The bill provided for “general exemptions” and “specific exemptions”. The specific exemptions in the bill were carried forward in similar form in sections 54 to 57.²
- 6.1.7 The Privacy of Information Bill would have enabled the Tribunal to grant general exemptions from all or any of the information privacy principles where satisfied that this was clearly in the public interest. The bill set limits on the granting of exemptions, and specified who might apply for them. If the Tribunal were to decide to grant an exemption it might itself formulate the exemption or, where it considered that the exemption should take the form of a code, refer the matter to the Commissioner for the purpose of preparing that code of practice. On finalising such a code the Commissioner would submit it to the Tribunal which would approve the code as an exemption, refuse to approve the code, or make modifications.
- 6.1.8 The Select Committee decided to remove the Tribunal from involvement in promulgating codes of practice. Instead, it placed with the Privacy Commissioner the functions of:
- issuing codes of practice (sections 46-53); and
 - granting specific exemptions (albeit in more restricted circumstances than were proposed for the Tribunal).³

¹ In 1996/97 I granted 25 authorisations but since 23 of these were in identical terms in respect of individual Crown Health Enterprises, it may be more meaningful to categorise these as amounting to just three authorisations.

² With the omission of one for “small clubs” which was dropped by the Select Committee.

³ Whereas the Tribunal would have been able to grant exemptions from any of the principles the Commissioner can, under section 54, exempt actions from only principles 2, 10 and 11.

6.1.9 One of the reasons for the Select Committee’s change was the near impossibility of adequately dealing with such issues in an adversarial hearing with multiple parties. Although the bill did provide that the Privacy Commissioner could have undertaken drafting at the request of the Tribunal the arrangements in the bill still appeared to be problematic. It also appeared inappropriate to have the body with final adjudicative powers on complaints, the Tribunal, also having the legislative role of producing codes of practice. The arrangements adopted by the Select Committee solved these problems and seem to bring other advantages into the process as well.

Why codes of practice?

6.1.10 The establishment of codes of practice under the Privacy Act is essentially a rule making exercise and the resultant codes are “secondary” or “delegated” legislation. Provision was made for delegated legislation codes of practice because dealing with everything by primary legislation, particularly “changing the rules”, is problematic. In particular:

- the process of promoting or changing Acts of Parliament is expensive, intricate and generally very slow;
- statutes are good for providing the broad outline of law but usually do not provide an appropriate vehicle for the detail of rule making due.

6.1.11 Codes of practice have been chosen by Parliament for delegated rule-making in a variety of circumstances in recent years. They are used in relation to building standards, workplace safety, health and disability services, and broadcasting standards amongst others. Advantages advanced for codes of practice over traditional regulations have included:

- the involvement of industry and the public in consultation and development of rules, sometimes a measure of self-regulation;
- a greater degree of flexibility than other methods of delegated or primary legislation.

6.1.12 However, codes of practice are not universally welcomed. Overseas critics have suggested:

- codes can lessen Parliament’s control over the setting of legal standards;
- codes create a risk that regulation will not be cost-effective;
- codes may not be as readily available to the public as Acts and regulations;
- the status and precise effects of codes are sometimes left unclear;
- codes can take a very long time to develop;
- codes can be used to avoid stronger laws which would better protect public or individual interests
- codes may not provide adequate remedies for complainants.

These criticisms have generally been made where the codes do not have the backing of legislation and where they have been produced to avoid regulation.

6.1.13 In conducting my review I have been careful to consider the merits and potential demerits of codes, as against other forms of rule-making. I have, for instance, borne in mind the potential for imposing compliance costs through codes of practice. However, the mechanism also has some potential for *reducing* compliance costs where appropriately used and it may be the aim of some codes to do so. The Act itself is already carefully structured to avoid some of the shortcomings of early codes of practice models - for example, the Act requires the code to be published and made available for purchase.

Role and placement of exemptions and exceptions

6.1.14 In considering the case to retain, limit or expand, the range of existing exemptions I have needed to carefully consider the role of exemptions and exceptions in a privacy law.

- 6.1.15 One of the prime features of the Privacy Act is its seamless application across public and private sectors. Where there are limits on its coverage, these are relatively constrained and do not create major anomalies. I am loathe to undermine this feature in any significant way - especially, of course, where that would detrimentally affect privacy. However, I have held myself open to be persuaded about cases for exemption since I would not wish the privacy law to be undermined, or made vastly more complicated, through its application to an inappropriate set of circumstances. This has been a consideration in my proposal for limiting the existing intelligence organisation exemption rather than eliminating it entirely.⁴ I consider that the application of the information privacy principles directly to the news media is inappropriate, in part for the same reason, although that issue arises under section 2 and not these provisions.⁵
- 6.1.16 The *location* of exemptions or exceptions can confuse users of the Act as we have:
- exceptions located in the privacy principles;⁶
 - exceptions located elsewhere in the Act or by reference to other legislation;⁷
 - provision for authorisation or exemption under section 54;
 - exemptions elsewhere in the Act;⁸
 - exemptions in codes of practice.⁹
- Accordingly, one matter I have considered is whether the exceptions and exemptions are appropriately located. A particular consideration in this regard is the need to make the Act more “user friendly” for the wide range of agencies to which the law applies. Elsewhere, I have, for instance, recommended that certain features of section 7 be relocated as exceptions directly into the relevant principles.¹⁰
- 6.1.17 I have also had to consider in this review whether *the Act* provides a suitable place to locate exemptions which could otherwise be issued by code of practice. I have concluded that amendment to the Act to provide for exemptions, notwithstanding the code provisions, is appropriate where:
- Parliamentary time will be engaged upon amendment to the Privacy Act in any case - as is likely to be the case with this review;
 - the subject matter is appropriately dealt with by primary legislation which, in a democracy, has the greatest status and legitimacy - I have in mind, for instance, that any exemptions would reduce citizens’ existing rights.¹¹
- However, some types of exemption would be unsuitable for including in the primary legislation. For example, if there would need to be a constant amendment of the provision, the Act may be the wrong place.¹²
- 6.1.18 Through certain other suggested amendments, such as recommendation 28 in relation to principle 12, I believe that any need for exemptions is diminished. For example, the exemptions provided in one code of practice will be rendered unnecessary if the changes to principle 12 are adopted.¹³

⁴ See paragraph 6.13 and recommendation 83.

⁵ See paragraphs 1.4.49 - 1.4.62.

⁶ See information privacy principles 2, 3, 10 and 11.

⁷ See sections 7 and 60. I make several recommendations for relocating the exemptions or exceptions in section 7 - see recommendations 30, 31, 32 and 33.

⁸ See sections 55-57.

⁹ See section 46.

¹⁰ See recommendations 30, 31 and 33.

¹¹ Indeed, section 46(5) expressly provides the code cannot reduce rights of access to personal information held in the public sector - as that was a right that existed prior to the Privacy Act and Parliament made it clear that it did not wish a Commissioner to limit those rights.

¹² Rules which might need to be constantly revisited, and amended, or containing very complicated administrative matters not carrying with them issues of high public policy, would seem unsuitable for direct amendment of the Act and might be left for codes.

¹³ See Superannuation Schemes Unique Identifier Code 1995.

SECTION BY SECTION DISCUSSION - Codes of practice

6.2 SECTION 46 - Codes of practice

6.2.1 Section 46 provides for the Commissioner to issue codes of practice. A code may modify the application of the information privacy principles by prescribing standards that may vary from those prescribed by the principles or by exempting particular actions from the principles. A code of practice may also prescribe how the principles are to be applied or complied with.

6.2.2 A code of practice may apply to:

- any specified information or class of information;
- any agency or class of agency;
- any activity or class of activity;
- any industry, profession, or calling, or class of industry, profession or calling.
- It may also regulate information matching in the private sector, set guidelines in respect of charges, and provide for various administrative and mechanical aspects of the code.

In connection with personal information held by public sector agencies, a code of practice may not limit or restrict the circumstances in which individuals may exercise their entitlements under principles 6 and 7.

6.2.3 Since 1993 I have issued six codes. Four of these remain in force (the other two having expired). Only one major sectoral code has been issued, the Health Information Privacy Code, with the others being modest, addressing quite particular issues. Two proposals for major codes remain before me relating to telecommunications network operators and credit reporting agencies.

6.2.4 The need for codes of practice has, with experience, proved to be less than some had expected. For example, when the bill was being enacted there was talk of codes of practice being necessary in relation to both the banking and insurance sectors. This has not proved to be the case.

6.2.5 There are a number of reasons which may explain why fewer codes have been issued than might have been expected:

- the perceived problems or issues which might have led some people to expect codes were ill-founded or have not been borne out by experience;
- the anticipated problems did exist but were adequately dealt with by amendments made to the Privacy of Information Bill by the Select Committee;
- the anticipated problems did exist but were of a relatively minor nature and have been resolved through agencies changing their practices to bring them into conformity with the principles;
- the perceived need for codes might have been based upon a fear that the principles might be interpreted in a particularly restrictive way. This has not been borne out in practice through the opinions rendered by the Privacy Commissioner, or the decisions of the Tribunal, or has yet to be tested through a real complaint;
- there may remain a case for a code of practice but it has not been possible to bring it to fruition perhaps through resourcing reasons either with the industry body or at the Commissioner's office;¹⁴
- a desire for a code exists but the legal authority to issue it in the form desired by the promoters does not exist.¹⁵

¹⁴ Certainly more progress would have been possible on the proposed credit reporting code, and the proposed telecommunications code, if the Commissioner's office had had the resource to devote to these two major projects. Progress on both has been stalled while resource is applied to this review.

¹⁵ An example would be the desire of the Accounting Standards Review Board to have their financial reporting standards prevail over information privacy principle 11. A code of practice was proposed as the vehicle to achieve this. However, this does not seem to be appropriate and consideration has instead been devoted to addressing the matter legislatively.

VI

s 46

207

“A huge amount of work, time and resources goes into developing a code of practice. The effect of this expense is seen in the small number of codes that have been drafted. Industries perceive minimal benefits to their consumers, the costs of drafting a code appear to outweigh the benefits. The result is an inaccessible and ineffective code mechanism.”

- NZ LAW SOCIETY PRIVACY

WORKING GROUP, SUBMISSION N16

“The lack of resources and resulting inability of the Commissioner’s Office to review and issue codes of practice in a timely manner negates the benefits of offering such a specialised mechanism within the Act.”

- NZ LAW SOCIETY
PRIVACY WORKING GROUP,
SUBMISSION N16

- 6.2.6 Section 46(2) is quite precise as to what a code of practice may do. Some people who have tried to develop a code for consideration by the Commissioner have been frustrated by the fact that this puts them into something of a “legal straitjacket”. Some have thought that a very simple document, presented in the form of a glossy leaflet and running to just a couple of pages, might “do the trick” for a code of practice. However, it has been essential for people who have wanted a code of practice to understand that the resultant code is *delegated legislation*. In other contexts codes of practice are used to simply:
- explain legal obligations; or
 - show a company’s policy on the matter under consideration; or
 - show a company’s commitment to something, such as privacy.
- There may be a good case to develop such documents. However, such documents are not the stuff of Privacy Act codes of practice. A privacy code alters the legal obligations imposed under statute and therefore must be issued with the precision one expects of legislation and remaining within the powers conferred by the Act on the Commissioner.
- 6.2.7 On legal advice I have developed a structure for codes of practice which meets the requirements of the section and is standardised for whatever code is issued. I have issued a guidance note which directs people who must prepare preliminary drafts to my requirements.¹⁶
- 6.2.8 I have a few recommendations for amendment to section 46 which mainly take account of amendments to the section, and to other statutes, since 1993. They are also directed towards ensuring codes can do the multitude of things that may be expected of them. The changes in particular are to:
- tidy up section 46(2)(aa) inserted in 1994;
 - permit a code of practice to do certain other specific things under subsection (4);
 - provide a somewhat more flexible subsection (6), noting in particular that a Health Information Privacy Code has now been issued.
- Section 46(2)(aa)*
- 6.2.9 The Privacy Amendment Act 1994 inserted paragraph (aa) in subsection (2). This provides that a code of practice may:
- “apply any one or more of the information privacy principles (but not all of those principles) without modification.”
- 6.2.10 The first code of practice, issued in 1993, modified various principles by prescribing standards that were more, or less, stringent than the existing principles and exempting some actions from the principles. I adopted the practice of issuing a code with twelve rules corresponding with the twelve information privacy principles. In some cases the rules simply repeated, with minor stylistic changes, the relevant information privacy principles. I took the view that for this sectoral code to be satisfactory it needed to contain all twelve of the principles so as to avoid a complicated situation whereby the operative provision might be the unmodified principle in the Act in some cases and the modified rule in the code in others. It was later suggested to me that there was a problem in including an unmodified principle in the code. Although the possibility of an agency taking that rather fanciful point seemed remote it could not be ignored since during the first three years remedies for interference with the privacy of an individual arising from a breach of certain of the principles were not available unless those breaches constituted a breach of a code of practice.¹⁷
- 6.2.11 Accordingly, section 46 was amended to include paragraph (aa) which made it

¹⁶ See Privacy Commissioner, Guidance Note on Drafting Codes of Practice under Part VI of the Privacy Act, 12 May 1997.

¹⁷ See section 79(3).

clear that a code could apply any one or more of the information privacy principles without modification. However, the Department of Justice insisted upon including within the provision the parenthetical phrase “but not all of those principles”. I did not support the inclusion of that phrase because it was premised on the unfounded notion that the Commissioner might issue codes containing 12 unmodified principles simply in order to ensure that remedies were available during the transitional phase during the Act’s first three years. From my point of view, this was never in prospect and, of course, it did not eventuate. However, now that the transitional provisions are over and there would be no point in issuing a code containing 12 unmodified principles, I recommend the deletion of the words in parentheses as unnecessary “clutter” which is now not needed, if it ever was. Leaving the words there simply means that anyone considering the section has to try to fathom the reasoning for such words, which is not apparent unless one also notes the relevance of section 79 which touches upon breaches of certain principles occurring before 1 July 1996.



RECOMMENDATION 73

Section 46(2)(aa) should be amended by deleting all of those words in parentheses, that is “but not all of those principles”.

Section 46(4)

6.2.12 Subsection (2) sets out in general the main things that a code of practice may do. Subsection (4) supplements this by listing further specific things that a code might also do. These essentially are to:

- (a) impose controls in relation to private sector information matching;
- (b) set guidelines for making charges for giving access or to prescribe circumstances in which no charge may be imposed;
- (c) describe procedures for dealing with complaints;
- (d) provide for the expiry of a code.

6.2.13 So far the provisions in (a) and (b)(i) have not been utilised. In the Health Information Privacy Code I did exercise the power in (b)(ii) to prescribe circumstances in which no charge may be imposed.¹⁸ There is a limit to the use that may be made of the provision prescribing complaints procedures provided for in paragraph (c). The power is tightly circumscribed as such provisions may not limit or restrict the provisions of Part VIII or Part IX of the Act. However, in the Health Information Privacy Code 1994 I included a clause providing that a health agency may designate a person or persons to deal with complaints alleging a breach of the code.¹⁹ Under paragraph (d) in the Health Information Privacy Code I provided for a review of that code - scheduled for next year.²⁰ In three codes I have included an expiry clause as provided for in paragraph (e).²¹

6.2.14 Some unrealistic expectations exist amongst agencies or organisations who have approached me to discuss the possibility of codes of practice. Some have thought that if there is a privacy problem, or a compliance problem, that I have a straightforward power to change any aspect of the law by code of practice. Clearly that is not the case and subsections (2) and (4) are restricted in what may be done by code of practice - and it is appropriate that this should be the case. Codes of practice will not be a panacea for all privacy or compliance issues.

¹⁸ See Health Information Privacy Code 1994 clause 6.

¹⁹ Health Information Privacy Code 1994, clause 8. That clause was accompanied by a commentary explaining features of complaints under the Privacy Act and the characteristics of a satisfactory internal complaints process. I am not confident that the clause has made much difference to the question of whether agencies are geared up to handle complaints. A standard model for internal complaints handling, or external industry complaints handling, is not possible because of the diversity of disciplines and agency type of the health sector.

²⁰ See Health Information Privacy Code, 1994, clause 2(2).

²¹ Both the Health Information Privacy Code 1993 (Temporary) and the GCS Information Privacy Code 1994 have expired. The EDS Information Privacy Code 1997 will expire on 30 June 2000.

“Existing codes follow the format and wording of the existing information privacy principles wherever possible. Given the convoluted nature of the existing principles, this makes the codes very difficult to understand for the average person. Lengthy explanatory notes do not assist. It would be preferable if codes were worded as simply as possible.”

- TELECOM NEW ZEALAND,
SUBMISSION N7

- 6.2.15 In some specific legislation it has been found desirable to permit certain explicit things to be done by a Privacy Act code of practice. Appendix G describes the provisions found in the Local Government Act 1974, Domestic Violence Act 1995 and Dog Control Act 1996. It so happens that each of those provisions touch upon *public register* codes of practice and I will deal with those elsewhere²² but it is possible that another statute could confer additional powers in relation to a section 46 code as well. It may be desirable to link section 46(4) to those other powers by a formulation indicating that a code may do anything authorised by another enactment.

**RECOMMENDATION 74**

Section 46(4) should be amended by adding a paragraph acknowledging that a code may provide for such other matters as specified in any other Act.

- 6.2.16 I suggest elsewhere in this report that certain other matters be dealt with by code of practice. These would probably be implemented by amending section 46(4).²³

Section 46(6) and (7)

- 6.2.17 Generally the information privacy principles apply only to information about *living* individuals. This is achieved through the definitions of “personal information” and “individual” in section 2. In particular, “individual” is defined to mean “a natural person, other than a deceased natural person.” However, the select committee studying the Privacy of Information Bill concluded that it would be necessary to make some protection in relation to medical records of deceased persons. There are undoubted sensitivities in the area and notions of medical confidentiality had always extended beyond a patient’s death.

- 6.2.18 It was decided that the general application of the principles should remain limited to personal information about living natural persons but that, in the event of a code of practice being issued in relation to health information, the law should extend to information about deceased persons. The select committee knew that it was my intention to develop a code of practice for the health sector as one of my first priorities. At the same time as the latter part of the committee’s study of the Privacy of Information Bill, there was also study by the Social Services Committee of amendments to the Health Act 1956 as part of the major health reforms. There was some co-ordination between the two legislative initiatives and, for instance, subsection (7) takes the same meaning of “health information” as had been devised for section 22B of the Health Act 1956.

- 6.12.19 The Health Information Privacy Code 1994 is now an established feature of the legislative landscape for dealing with health information in the health and disabilities sector. Subsections (6) and (7) necessarily speak in the abstract of the “issuing under the section of any code of practice relating to health information” that makes it clear that it “shall be read as if it applies in respect of health information about any individual, whether living or deceased.” In my view, the provision should now be revisited so as to narrow its effect and to recast it as a power which the Commissioner may exercise rather than an automatic effect.

- 6.2.20 At present, if I issue a code of practice relating to “health information”, as defined in section 22B of the Health Act, that code is to be read as if it applies to information about deceased persons. I foresee several problems with this if it is taken to its logical conclusion:
- section 46(6) is not limited to health information *held by health agencies* (whereas this is the application of the Health Information Privacy Code and the primary application of Health Act itself);
 - the code is to be read as if it applies to deceased persons whatever the code

²² See paragraph 7.12.

²³ See recommendations 18, 27 and 35(b).



Bruce Slane and Blair Stewart: the Privacy Commissioner and Manager, Codes and Legislation, confer over the issue of the Health Information Privacy Code 1994.

PHOTO: OFFICE OF THE PRIVACY COMMISSIONER

otherwise says (and therefore the provision in the code that purports to limit rule twelve to health information for twenty years after death may not be effective);

- any other code which relates to “health information” will extend to such information about deceased persons.²⁴

- 6.2.21 It seems to me desirable that subsections (6) and (7) be changed so that a more flexible provision, potentially applying to a far more limited class of cases, is created. The essential feature is that it should be clear that a code of practice *may* apply principle 11 to “health information” about deceased persons. I tried to strike a balance by applying the Health Information Privacy Code to information about deceased persons for up to twenty years beyond their death only (although as noted that may be ineffective). Accordingly, I suggest that the Commissioner should be able to provide that a code may apply principle 11 to health information about deceased persons for such period beyond the person’s death as prescribed in that code of practice. If this were to be adopted I would schedule an amendment to the Health Information Privacy Code 1994 to align the code with the new provision in the Act.



RECOMMENDATION 75

Section 46(6) should be replaced with a provision which empowers the Privacy Commissioner to include in a code of practice a provision applying principle 11 to an agency, or a class of agencies, to health information about any deceased person for a period specified in the code beyond any such person’s death.

6.3 SECTION 47 - Proposal for issuing code of practice

- 6.3.1 Section 47 provides that I am empowered to issue a code of practice on my own initiative or on the application of any person. An application for a code may only be made by a person that has the function of representing the interests of any class or classes of agency, or of any industry, profession, or calling, and where the code sought is intended to apply in respect of the entities represented by that body. Where any such application is made, I am required to give public notice that the details of the code sought may be obtained from the Commissioner and that written submissions may be made within the period specified in the notice.

Representative body applications

- 6.3.2 To date no codes of practice have been processed on the basis of an application to the Commissioner by a “representative body”. Although many of the codes have had a promoter who has undertaken some drafting, facilitated some preliminary non-statutory consultation, and produced the draft to me, none has formally applied under section 47(2). Each has been content to provide a draft code and encourage me to initiate the process under section 48.
- 6.3.3 For example, the (then) Department of Health undertook some preliminary work on the proposed Health Information Privacy Code, but the draft code produced was not given to me in the capacity as a “representative body”. The Association of Superannuation Funds of New Zealand (ASFONZ) played a leading role in promoting the need for a code of practice which eventuated as the Superannuation Schemes Unique Identifier Code 1995. However, in that case my own office undertook the drafting. In respect of the Justice Sector Unique Identifier Code 1998 the Ministry of Justice, as part of its co-ordination role for the Justice Sector Information Committee, produced to me a draft which developed as a Commissioner-initiated code. With respect to proposed codes in the credit reporting and

“Given the time and resource constraints on the Commissioner’s Office, and the inordinate delays this produces in the issuing of codes, section 46 should be amended to permit agencies to issue codes of practice subject to a public notification procedure. The Commissioner should then have the ability to amend such codes (again through a public notification procedure) within a period prescribed under the Act.”

- TELECOM NEW ZEALAND,
SUBMISSION N7

²⁴ An example would be a code of practice applying to all personal information in the hands of a class of agencies. If that included, say, medical reports that might be held by an employer or insurance company, this might mean that principle 11 would have to read as applying to both living and deceased persons.

telecommunications areas I have had drafts presented to me by, respectively, an industry group of credit reporting agencies, a major credit reporting agency, and a working group of three major telecommunications network operators. None has claimed “representative body” status.

- 6.3.4 In each of the cases where codes have been issued so far the process has worked satisfactorily. The resultant status of a code is unaffected by whether it is initiated by the Commissioner or a representative body. However, it may be that the restrictions upon representative body applications limit the potential of the process. At present, I have no direct experience to draw upon because none of the relevant bodies has put the matter to the test. However, if we take the case of the proposed credit reporting and telecommunications codes, the fact is that I received draft codes some considerable time ago and have not myself initiated the statutory processes as yet. My decision has been based on a variety of matters including my own priorities and resources. On the other hand, the industries concerned might feel that they would have preferred to have had their draft code publicly notified by now (notwithstanding that I would not be bound, regardless of the outcome of the section 47(2) process, to issue the code).
- 6.3.5 Accordingly, I have considered whether it might be possible to relax some of the constraints provided for in subsection (3).
- 6.3.6 There are few bodies in New Zealand which could truly be said to represent *all* of a particular class of agency or of any industry, profession or calling. Probably the only bodies which could sustain such a claim represent regulated professions whereby to practice a person must be a member of the body. However, although the matter has not been tested, it should not be assumed that section 47(3) is intended to be read so restrictively. The key test is that the applicant body must have the purpose, either alone or with other purposes, of representing the interests of a class or classes of agency or an industry, profession or calling. On this approach it would probably be the case that in the examples quoted above that ASFONZ would likely fall within the ambit of section 47(3) but that the individual credit reporting agency, telecommunications working group and the Ministry of Health would not.
- 6.3.7 It would be possible to put the matter beyond doubt by adding the words “or a substantial section of” to line two of section 47(3)(a). I simply make this as a suggestion for consideration since I have not yet had the opportunity to consider the matter in a real case. However, the important thing is that subsection (3) must not be too rigid if it is to achieve its original objective (notwithstanding that reliance upon Commissioner-initiated codes has largely worked satisfactorily for industry groups to date).
- 6.3.8 Section 47(2) was never geared to applications by public sector agencies. Although not expressly excluded, such bodies would rarely if ever have the necessary representative status. Although two public sector agencies promoted two codes to me, which were eventually issued, I received no submissions suggesting that section 47(3) should be redrafted to encompass departments or other public sector agencies.²⁵ I see no particular need for change in this respect since the Commissioner-initiated route has appeared satisfactory to date.



RECOMMENDATION 76

Consideration should be given to amending section 47(3) to make it clear that a body can apply for a code whether it represents the whole of a class of agencies, industry, profession etc or just a substantial section.

²⁵ The Health Department, as it then was, did some initial drafting and consultation on the Health Information Privacy Code 1994 and the Ministry of Justice promoted what became the Justice Sector Unique Identifier Code 1998.

“Section 47(3) should be revoked. If section 47(3) is retained then it should be made clear that where some major players in an industry have been given the opportunity to participate in the preparation of a code, but have declined to do so, this should not prevent the remaining majority of players from being treated as representative of that industry.”

- TELECOM NEW ZEALAND,
SUBMISSION N7

Costs of section 47(2) applications

- 6.3.9 There are many calls on the resources of my office. Other than the Health Information Privacy Code, a major sectoral code, the codes of practice issued so far have not been a big cost item although two codes in prospect, relating to credit reporting and telecommunications, will be significant initiatives when they are taken forward. Nonetheless, there is a basic cost in publicly notifying any application.
- 6.3.10 I have also found that some sectors bring forward proposals which “jump the queue” and upset priorities that I have myself established. An example is the Justice Sector Unique Identifier Code 1998 which was an initiative from the law enforcement sector being driven by the needs of those agencies and the timing for their migration off the Wanganui computer system. I consider that there is a case to be made for an application fee, or a cost recovery process, for such code proposals.
- 6.3.11 It would be possible for the Commissioner to negotiate with an applicant for a contribution to costs. Such arrangements are informal and voluntary. They remain open to criticism of the Commissioner, pressure on the Commissioner to approve a code in the form designed by an applicant, and allegations of unfairness as between the treatment of different applicants. For example, a request for a voluntary monetary contribution in cases of urgency skews the process. What the applicant considers urgent may not in fact be so. Priorities should normally be determined having regard to the urgency of all matters before the Commissioner, viewed objectively. I might add, by way of illustration, that I did seek a contribution from the Ministry of Justice towards the costs of processing the Justice Sector Unique Identifier Code for which urgency was claimed. My intention had been for such contribution to meet the costs of public notices and purchase legal resource from a barrister to replace staff-time diverted to the project. No contribution was forthcoming.
- 6.3.12 Provision should be made to at least defray the costs of notifying a section 47(4) application. Public notification costs for a code typically run to about \$600-\$800. I suggest that the Act should provide that the Commissioner may require the applicant itself to publicly notify the application in terms directed by the Commissioner.

**RECOMMENDATION 77**

There should be provision for the Commissioner to require a representative body applicant to undertake notification under section 47(4) in terms directed by the Commissioner.

Section 47(5)

- 6.3.13 I suggest that section 47(5) be repealed. Presently this provides that the publication of a notice under section 47(4), concerning a representative body application, is sufficient compliance with the requirements of section 48(1)(a), concerning notification of the Commissioner’s intention to issue a code. In my view, it may be better for representative body applications to be notified, together with consultation on the representative body’s proposal, and *then* for that to be followed, if the proposal warrants it, with section 48 notification of the Commissioner’s intention to issue a code. It is highly unlikely that the proposed code put before the Commissioner by a representative body will be satisfactory to the Commissioner in all respects. A change of some sort is inevitable and, if experience of the first few years of operation of the Act is to be repeated, then the draft codes brought to the Commissioner will generally require substantial - even fundamental - change to be satisfactory.
- 6.3.14 If there is to be substantial change to the codes submitted by the representative body then it may be unsatisfactory to finally issue a revised version without

further notification. While any redrafted code would be the subject of further discussion with the representative body this would not necessarily bring the changes to the attention of all others who may have an interest and who would like to be consulted (although section 48(1)(b) also imposes some further steps to be taken in that regard). The problem I foresee is similar to that experienced occasionally by select committees. When bills are reported back in a hugely changed form, criticism can be made that the bill is no longer the one that interested persons had a chance to consider and make submissions on.

- 6.3.15 It should also be borne in mind that a considerable time can elapse between a representative body proposal being received by the Commissioner and publicly notified and the time at which the Commissioner eventually issues a code. New players may enter the scene in the meantime. Regardless of whether significant substantive change has been made to the draft in the meantime it is probably undesirable for a new code to arrive unheralded by a public notice showing the Commissioner's intention to proceed with the issuing of the code.
- 6.3.16 It is wrong to suppose that the public notification of a representative body proposal should be sufficient as a section 48(1)(a) notice. Notification under section 47(4) is, to my mind, an entirely neutral process whereby the Commissioner simply indicates that an application has been received. It expresses no view on the merits of the proposal and indeed it is conceivable that the draft code before the Commissioner has never previously been seen or considered by him. On the other hand, a section 48(1)(a) notice gives interested persons an indication that the Commissioner *intends to issue* the code. That is, that the Commissioner has in general terms taken a preliminary position on the broad matter (although, of course, he will be willing to be persuaded on the detail).
- 6.3.17 My solution is simply to repeal section 47(5). No other change is necessary. The result will be that with a successful representative body application there will be two public notices. The first indicating that an application has been received and that the draft code prepared by the representative body is available for consideration and for submission. The second notice will indicate that a proposed code is available, quite possibly different from the representative body's, and commencing full scale consultation.



RECOMMENDATION 78

Section 47(5) should be repealed.

6.4 SECTION 48 - Notification of intention to issue code

- 6.4.1 This provision makes it clear that I must not issue a code of practice unless I have:
- given public notice of my intention to issue the code;
 - done everything reasonably possible to advise all affected persons, or representatives of those persons, in relation to the proposed code, and invited submissions.
- 6.4.2 The emphasis of the section is to reach out to find affected persons, make them aware of the proposed code, and seek their views. It is clear that Parliament does not expect the Commissioner to place a couple of public notices and leave matters there. It enjoins him to “do everything possible to advise all persons who will be affected” and subsection (3) notes that nothing in subsection (1) prevents the Commissioner from adopting any *additional* means of publicising the proposal.
- 6.4.3 In addition to placing public notices in newspapers in four or five main centres, I typically take the following steps in relation to a proposed code:
- issue a media release;

- refer to the proposal in my own regular newsletter *Private Word*;
- develop a mailing list and send copies of an explanatory statement and a copy of the proposed code to persons who might be affected or interested;
- ask the promoter of any code proposal to contribute suggestions as to persons to consult with;
- encourage the matter to be reported in appropriate trade journals.²⁶

6.4.4 I have adopted the practice in public notices of including the freephone number of the Privacy hotline from which copies of the proposed code may be obtained. Copies are also available by mail or fax or can be requested by e-mail. My web site is also available for dissemination.

6.4.5 The period allowed for consultation will depend upon the urgency of the matter and the numbers of persons likely to be interested or affected. The period normally ranges from one to two months.

6.4.6 The submissions are acknowledged and then compiled for my information and that of staff working on the code proposal. Where there are a significant number of submissions, an analysis may be prepared to assist with considering the points raised. With the larger code consultations I have held consultation meetings. In respect of the Superannuation Schemes Unique Identifier Code 1995 I held a meeting in Wellington. In respect of the Health Information Privacy Code 1994 I held a number of consultation meetings in the four main centres.

6.4.7 Frequently where submissions raise important points which require further elaboration or clarification, my staff will write to the person making the submission seeking a supplementary submission. Sometimes matters are simply clarified on the telephone. I have also adopted a practice of canvassing certain well informed “stakeholders” on proposals for inclusion in codes both before a code is released for public consultation and during that process. After the code has been issued I have always encouraged affected persons to let me know if the code is causing any difficulties in operation. Sometimes the printed code includes a statement to this effect.

6.4.8 Undoubtedly consultation is at the heart of the code of practice provisions. This is formally initiated by public notification and therefore section 48 is a key provision. I consider the section to have operated satisfactorily and recommend no change.

6.5 SECTION 49 - Notification, availability and commencement of code

6.5.1 This section provides that where the Commissioner issues a code of practice, a notice, to the effect that the code is in place and stating that copies are available, must be published in the *Gazette* as soon as practicable. The Commissioner must ensure that copies of the code are available for inspection and purchase at a reasonable price for so long as the code remains in force. A code may not come into force earlier than the 28th day after its notification in the *Gazette*.

6.5.2 As earlier noted, statutory codes of practice are a relatively modern creation and represent a departure from the traditional forms of delegated legislation such as regulations or by-laws. Adequate access to all forms of law is essential if citizens are to know the legal rules by which they are bound. One of the criticisms that has been levelled overseas at codes of practice is that people sometimes do not hear of the fact that they have been issued and that they can be hard to obtain.

²⁶ In relation to the recent Justice Sector Unique Identifier Code the matter was, for example, reported in the newsletter of the NZ Police, *Ten-One*.

I do not believe that this has been the case in relation to codes of practice issued under the Privacy Act and section 49 is a key provision to ensure that that does not happen in the future.

- 6.5.3 Following notification in the *Gazette* I typically take some or all of the following steps to make the code available:
- send a copy to anyone who made a submission on the proposed code;
 - issue a media release;
 - post the code onto my Internet site;
 - make the code available for purchase from my office, and from Bennett’s GP Bookstores, at a reasonable price;
 - made the code available for inspection at my office;
 - deposit copies in the National Library;
 - distribute copies to the depository libraries;
 - notify key stakeholders of the issue of the code;
 - note the issue of the code in *Private Word*;
 - co-operate with commercial publishers in relation to their plans for republishing the code in practitioner texts.

- 6.5.4 In 1996 the Regulations Review Committee of Parliament reported on the results of an investigation into access to regulations. The focus of the Committee’s recommendations was the public availability of delegated legislation which are “regulations” in terms of the Regulations (Disallowance) Act 1989 but which are not published in the traditional “SR” (Statutory Regulations) series. This includes certain types of regulations such as Ministerial “rules” and accounting standards and, in this context, codes of practice under the Privacy Act.

- 6.5.5 The Committee was keen that steps be taken to make the less traditional forms of delegated legislation easily available to the public. I am pleased that a Parliamentary committee has taken an interest in the matter since undoubtedly access to certain official publications has become more complicated with the various public sector restructurings, the privatisation of the Government printing office and the closure of the Link Centres. Nonetheless, some of the difficulties in obtaining other types of delegated legislation do not, in my opinion, apply in respect of codes of practice under the Privacy Act. I am not aware of any amendments that could be made to section 49 to enhance availability of codes since the provision would seem to adequately achieve the job as it is.

6.6 SECTION 50 - Codes deemed to be regulations for purposes of disallowance

- 6.6.1 Codes of practice issued under section 46 are deemed to be regulations for the purposes of the Regulations (Disallowance) Act 1989 but not for the purposes of the Acts and Regulations Publication Act 1989.

- 6.6.2 Section 4 of the Regulations (Disallowance) Act 1989 requires that codes of practice be laid before the House of Representatives within the sixteenth sitting day after the day on which they are issued. The House has the power to disallow any code of practice or provision thereof by resolution under section 5 of the 1989 Act. The codes have been laid before Parliament but there has been no disallowance as yet.

- 6.6.3 The existence of disallowance processes is probably of greater benefit to agencies than to individuals. Should they be dissatisfied at stricter controls, or at a failure to exempt some action, in a code they can approach any MP to take up the issue.

- 6.6.4 The Regulations (Disallowance) Act complements the functions of the Regulations Review Committee which presently operates under Standing Orders 195-198.²⁷ In addition to providing copies of codes for tabling I have taken it upon

“The Committee commends the Office of the Privacy Commissioner on the plain language drafting of the Code and on your comprehensive response to the Committee’s enquiries.”

- RT HON JONATHAN HUNT,
CHAIRMAN REGULATIONS REVIEW
COMMITTEE, ON A REVIEW OF THE
JUSTICE SECTOR UNIQUE IDENTIFIER
CODE 1998, JUNE 1998

myself to send copies directly to the Chairman of the Regulations Review Committee.

- 6.6.5 At present it is doubtful that the Acts Interpretation Act 1924 applies to codes of practice. This will change when the Interpretation Bill, presently before Parliament, is enacted. As codes are, by virtue of section 50, “regulations” for the purposes of the Regulation (Disallowance) Act, they will also be “regulations”, and hence “enactments”, for the purposes of the new Interpretation Act. This change would be of positive benefit for consistent interpretation of various codes and the Act.²⁸

6.7 SECTION 51 - Amendment and revocation of codes

- 6.7.1 Section 51 provides the Commissioner may amend or revoke a code practice issued under section 46, in which case the notice, publication and other requirements of sections 47-50 will apply. I have utilised this provision in making several amendments to the Health Information Privacy Code 1993 (Temporary) and later the Health Information Privacy Code 1994. None of the other codes have been amended and I have not, as yet, exercised the revocation power.

6.8 SECTION 52 - Urgent issue of code

- 6.8.1 This provision allows for the issuing, amendment, and revocation of codes where the Commissioner considers that following the notification procedure set out in section 46 would be impracticable because it is necessary to take action urgently. This involves a departure from the notice and consultation processes that would normally be expected. Therefore, as a safeguard, the code may remain in force for no longer than one year.
- 6.8.2 The only code issued under the urgency provisions was the Health Information Privacy Code 1993 (Temporary). This code was issued on 30 July 1993 within a month of the Act coming into force. Consultations with officials and others in the health sector in the lead up to the enactment of the Privacy Act had convinced me that health information privacy issues would need to be a priority and that a code would be warranted. I confirmed this after the Act was passed and determined that a code needed to be urgently finalised and issued. The code was initially intended to expire 11 months later but in 1994 I extended its duration, again using the urgency provisions, for a further month to enable completion of work on the Health Information Privacy Code 1994.
- 6.8.3 The period of operation of the temporary code provided good opportunity for a review to be carried out of its operation and for extensive consultation to be engaged in relation to its replacement, the Health Information Privacy Code 1994. The urgency provisions were found to be entirely satisfactory in these processes.
- 6.8.4 There was one other set of circumstances in which I considered using the urgency provisions. New Zealand’s first major piece of privacy legislation was the Wanganui Computer Centre Act 1976. It was directed towards “big brother” concerns arising from the operation of a law enforcement computer system. The aim of the 1976 Act was to ensure that the computer-based information system made no unwarranted intrusion upon the privacy of individuals. That Act was repealed with the Privacy Act 1993 and I have had some continuing interest and responsibilities in relation to it.²⁹

²⁷ *Standing Orders of the House of Representatives*, September 1996.

²⁸ See Report of the Privacy Commissioner to the Minister of Justice on the Interpretation Bill, December 1997.

²⁹ Aspects of the Wanganui system, the 1976 legislation and the issues arising from its repeal, are discussed in relation to Parts XI and XII of the Act. See paragraphs 11.1 - 11.6, 12.18.6 - 12.18.13 and 12.19 - 12.21. See also paragraph 10.1.18.

6.8.5 Once the Privacy Act was passed there was no need for a specific stand-alone piece of privacy legislation relating solely to one computer facility. However, that is not to say that privacy concerns in relation to the law enforcement database had diminished or disappeared. In recent years the Wanganui computer system had been operated by a state-owned company, GCS Limited. It also provided other computer processing to government agencies such as IRD.

6.8.6 With the enactment of comprehensive privacy legislation the government looked at selling its shareholding in GCS, a step that it had earlier considered but chosen not to pursue until privacy legislation was enacted. In mid-1994 the government announced its intention to privatise the company. In light of the historical concern shown in relation to the Wanganui computer centre, and the sensitivity of the information processed there and elsewhere by GCS, I announced my intention to issue a code of practice in relation to the company. The main purpose of the code was to ensure that there would be remedies for any breaches of the privacy principles - breach of some of which would carry no remedies, in the absence of a code, during the transitional phase of the Act. I also wished to ensure some privacy protection in the event that any of the information was to be transferred off-shore for processing. A tight time frame was in prospect because of the “due diligence” and sales processes.

6.8.7 Despite the tight time frames I am pleased to say that the code was developed and issued ahead of schedule and following full consultation. There was no need, in that instance, to rely upon the urgency provisions which would have diminished public notice or consultation.

6.8.8 The provisions for the urgent issue of a temporary code are an essential feature of the codes provisions. I believe the provision has worked well, adequately protects the interests of the public and agencies and does not need amendment.

6.9 SECTION 53 - Effect of code

6.9.1 Section 53 sets out the two main legal effects of a code of practice. First, any “action” (which also includes policies or practices) which would otherwise breach an information privacy principle is deemed not to breach that principle if done in accordance with that code. Second, failure to comply with the code, even if not otherwise a breach of a principle, is deemed to be a breach of a principle.

6.9.2 The effect of section 54 seems plain enough. Through reliance upon section 53 it has been unnecessary in section 66 to mention a breach of a code of practice issued under section 46 as constituting part of an “interference with the privacy of an individual” - the deeming provision means it is already there in the reference to any breach of an information privacy principle.

SECTION BY SECTION DISCUSSION - Specific exemptions

6.10 SECTION 54 - Commissioner may authorise collection, use, or disclosure of personal information

6.10.1 Section 54 is the first of 4 sections which set out certain specific exemptions. These include:

- *section 54*, which empowers the Commissioner to authorise the collection, use or disclosure of personal information which would otherwise be in breach of principles 2, 10 or 11, in the public interest or the interest of the individual concerned;
- *section 55*, which provides that nothing in principles 6 or 7 apply in respect of certain specified personal information;
- *section 56*, which provides an exception from the principles where the agency concerned is an individual and the relevant information is collected or held

“I express my thanks for the efficient and co-operative way in which the whole matter (authorisation) was handled. To the extent that conditions were imposed on what we were asking for, they were, to my eye, common-sense provisions which would ensure that the dissemination of personal information was kept to a minimum to achieve the Trustee’s purpose.”

- BUDDLE FINDLAY,
SUBMISSION N5

for the purposes of, or in connection with, that individual’s personal, family or household affairs;

- *section 57*, which exempts intelligence organisations from principles 1 to 5 and 8 to 11.

Section 54

- 6.10.2 Section 54 allows the Privacy Commissioner to specifically authorise an agency to collect, use, or disclose, personal information where it would otherwise constitute a breach of principles 2, 10 or 11. However, the Commissioner must first be satisfied that, in the special circumstances of the case, there is either a countervailing public interest, or else a clear benefit to the individual concerned, that outweighs any interference with privacy that could result from the breach of the relevant principle. The Commissioner may not grant such an authorisation if the individual concerned has refused to authorise the relevant collection, use or disclosure.
- 6.10.3 Occasionally allegations are made that the Privacy Act has prevented something which may have been desirable “in the public interest”. Section 54 exemptions are available to avoid this. I have released a guidance note to help agencies frame applications under the provision.³⁰ So far, few applications under section 54 have been received.
- 6.10.4 The section has an importance in that it provides a “safety valve” for exceptional cases. The exemption power is complementary to the code of practice power since it will not be feasible or desirable to issue an entire code of practice for “one-off” situations. It also has a role in easing compliance costs since in those circumstances where an exemption is justified it may save an agency from unattractive or costly alternatives such as foregoing a particular opportunity, obtaining specific statutory authorisation or pursuing a code of practice.
- 6.10.5 The power for the Commissioner to grant exemptions under section 54 is circumscribed. One issue therefore is whether the exemption power might usefully be broadened. Although the Commissioner may only give exemptions from principles 2, 10 and 11, it is interesting to note that the Australian Privacy Commissioner has powers to grant exemptions (referred to as “public interest determinations”) from *all* of the Australian information privacy principles.³¹ On the other hand, the Australian Commissioner has no power to issue codes of practice and it may be that the broad exemption power is intended to cover situations which codes of practice might address under our Act.
- 6.10.6 No application has yet been refused on the grounds of the weighting to be given to the public interest. I received one submission calling for greater weight to be given to the public interest in section 54 (submission N13). However, I believe the balance is correctly struck. In circumstances where it is appropriate for the public interest to prevail over the expressed wishes of the individuals concerned, I think a specific law, or a code of practice, are the appropriate means to achieve that and not an exemption granted by the Commissioner.

Extension to principle 9

- 6.10.7 In my view, there is a good case to extend the section 54 exemption power to authorise, in certain circumstances, departures from principle 9. Provision for exemption in these circumstances may contribute to resolving one-off compliance difficulties without the need to pursue codes of practice.
- 6.10.8 I see little difficulty in including reference to principle 9 in section 54 and do

³⁰ Office of the Privacy Commissioner, Guidance note to applicants seeking exemption under section 54 of the Privacy Act 1993, 12 May 1997.

³¹ Privacy Act 1988 (Australia), Part VI.

“Section 54(a) requires that the public interest outweigh ‘to a substantial degree’ any interference with the privacy of individuals and section 54(b) goes on to state that disclosure must involve ‘a clear benefit to the individual concerned’ that outweighs any interference with the privacy of the individual. This balance is drawn too close to the interests of privacy rather than those related to the interests of disclosure which might go some way to explaining why exemptions have been granted so rarely. If the public interest outweighs the interest of privacy then exemptions should automatically follow without any further reference to the weighing of the two competing interests.”

- COMMONWEALTH PRESS UNION,
SUBMISSION N13

not believe that the various tests and restrictions need be altered. One circumstance in which it might be useful is where certain personal information which is not available for further lawful use is mixed with, or attached to, other personal or non-personal information which can be used, and it is not feasible to detach the information.



RECOMMENDATION 79

Section 54(1) should be amended to enable the Commissioner to grant an exemption to enable information to be kept notwithstanding that this would otherwise be in breach of principle 9.

Public notification costs

- 6.10.9 A number of exemptions granted so far have included a condition that the applicant undertake public notification to make affected individuals aware of the exemption or the unusual collection, use or disclosure of personal information. This public notification has been undertaken by, and at the cost of, the applicant. This is simply achieved by the Commissioner imposing conditions provided for in section 54(2).
- 6.10.10 So far, I have not undertaken public notification of an application for an exemption although I anticipate that this would be appropriate in certain circumstances particularly where the exemption would affect a large class of individuals. I note that the Australian Privacy Commissioner is obliged to give public notice of all applications for public interest determinations that are received.³² I see no need to alter the New Zealand procedure to require publication in every case since often public notice will not be warranted. However, I suggest that in appropriate cases I should be empowered to require the applicant to publicly notify an application. This may especially be relevant with the extension of the exemption power to principle 9 since such application could involve retaining holdings of information in respect of whole classes of individuals.



RECOMMENDATION 80

Section 54 should provide that the Commissioner may require the applicant to publicly notify an application in appropriate terms.

6.11 SECTION 55 - Certain personal information excluded

- 6.11.1 Section 55 provides that nothing in principles 6 or 7 applies in respect of certain classes of listed information. If information falls within one of those classes an individual cannot exercise any rights of access or correction in respect of that information.
- 6.11.2 The first class of information excluded is personal information in the course of transmission by post, telegram, fax, electronic mail, etc. It would seem self-evidently undesirable to permit access or correction requests in respect of information in the course of transmission. In the absence of such an exclusion it would have been necessary to interpret other concepts in the Act to ensure the same result - for instance, by concluding that a postal operator does not really “hold” personal information contained in the letters that it carries.
- 6.11.3 The second and third categories of information excluded relate to evidence given, or submissions made, to royal commissions, commissions of inquiry and certain other inquiries. These exemptions are a little more controversial than the others since they do something that the Official Information Act and Privacy Act usually avoid, which is to declare an entire class of document “off limits” to access without taking a case by case approach.

“The power to grant exemptions should be extended to cover any of the principles. The power to issue codes does not remove the need for an ability to grant exemptions. Exemptions should be used as an alternative to the cumbersome procedure to issue a code of practice where the exemption is unlikely to affect anyone’s interests adversely.”

- TELECOM NEW ZEALAND,
SUBMISSION N7

³² Privacy Act 1988 (Australia), section 74(1).

- 6.11.4 The fourth and fifth exceptions are directed towards ensuring that investigations by the Privacy Commissioner (and the equivalent investigations which were formerly carried out by the Ombudsmen under the Official Information Act) can be conducted satisfactorily. This ensures that correspondence between the Commissioner and an agency whose decision is being reviewed is not itself the subject of access and correction rights.
- 6.11.5 It would be possible to amend section 55 by narrowing any of the existing exemptions. Alternatively, a case might be made to include new classes of information. A very good case would need to be made to include new exemptions since this would narrow rights that individuals presently enjoy. A particularly strong case would need to be made to exclude further information held in the public sector since such a provision would narrow access rights that had existed for up to fourteen years (and furthermore it would be somewhat pointless to exclude information from personal access under principle 6 if information could nonetheless be accessed by other people under the Official Information Act).
- Royal Commissions and commissions of inquiry*
- 6.11.6 Most people making submissions were content that the current exemptions be left as they are. However, several did express concern in relation to the breadth of exclusion (b) which concerns evidence given or submissions made to:
- a Royal Commission; or
 - a commission of inquiry.
- For example, submission N8 suggested that the exclusions should not be applicable if the evidence or submissions have been given in hearings open to the public.
- 6.11.7 These exclusions are derived from exceptions to the definition of “official information” in the Official Information Act 1982³³ which in turn is derived from the draft bill prepared by the “Danks Committee”.³⁴ However, the Danks Committee regarded the question of access to information held by Courts and judicial bodies (including commissions of inquiry) and local authorities to be outside its terms of reference and it expressly noted that it had not given any consideration to the matter.
- 6.11.8 The exceptions relating to Royal Commissions and commissions of inquiry apply only:
- “at any time before the report of the Royal Commission or commission of inquiry has been published or, in the case of evidence of submissions given or made in the course of a sitting open to the public, at any time before the Royal Commission or commission of inquiry has reported to the Governor-General.”³⁵
- 6.11.9 Therefore the individual concerned can seek access to evidence or submissions about him or her after that time - this is a right not afforded to other third parties under the Official Information Act generally.³⁶
- 6.11.10 I consider it important that individuals should be able to access evidence given, or submissions made, to inquiries which is personal information about them, and the Act allows for this - albeit after a commission has reported. It may be possible to consider a narrowing of the exception so as to enable access to be

³³ Official Information Act 1982, section 2 (definition of “official information”, paragraph (h)).

³⁴ Committee on Official Information, *Towards Open Government: Supplementary Report*, 1981, pages 63-64.

³⁵ See section 55(b).

³⁶ See Official Information Act 1982, section 2, definition of “official information”, paragraph (h).

sought to evidence given, or submissions made, in a public hearing notwithstanding that the inquiry had not yet reported.³⁷ This may be at some inconvenience to a Royal Commission or commission of inquiry but may be seen as consistent with other moves over recent years to enhance rights of natural justice. I recommend that narrowing the exception should be considered.



RECOMMENDATION 81

Consideration should be given to the desirability of narrowing section 55(b) so as to enable access requests by the individual concerned to evidence given, or submissions made, to a Royal Commission prior to the report to the Governor-General where that evidence was given, or the submissions made, in open public hearing.

6.12 SECTION 56 - Personal information relating to domestic affairs

6.12.1 Section 56 establishes an exemption in respect of personal information that is collected or held by an agency that is an individual where the information selected is held by that individual “solely or principally for the purposes of, or in connection with, that individual’s personal, family, or household affairs”.

6.12.2 This provision is based upon an exemption in the Data Protection Act 1984 (UK). However, section 56 is broader than the UK exemption since it relates to information “solely or principally” held in connection with an individual’s personal, family, or household affairs. The UK exemption applies to data concerned “only” with the “management of” such affairs.

6.12.3 The Hong Kong privacy law has adopted an exemption based upon the UK model but in addition to “personal, family, or household affairs” the Hong Kong provision exempts personal data held by an individual only for “recreational purposes”.³⁸ The UK has drawn upon the Hong Kong provision in the domestic purposes exemption in its new bill which provides:

“Personal data processed by an individual only for the purposes of that individual’s personal, family or household affairs (including recreational purposes) are exempt from the data protection principles and the provisions of Part II and III.”³⁹

6.12.4 I have considered the new Hong Kong and UK provisions but do not recommend change at this time. The absence of an express reference to an individual’s “recreational” purposes has not caused any difficulties in New Zealand, to my knowledge. As already observed, the New Zealand provision is already broader than the UK or Hong Kong models since the exemption in section 56 refers to “solely or principally” rather than “only”. I do not see any present case for broadening it further.

6.12.5 Some problems have been encountered where members of a family or household engage in misleading conduct. The most common example is where an estranged spouse or partner misrepresents to an agency that he or she is entitled to have access to personal information held about the other spouse or partner. In other cases, individuals have impersonated other family members to agencies.

6.12.6 In the discussion paper I questioned whether it is appropriate to allow individuals to rely on an exemption when they are engaging in misleading conduct with outside agencies to the detriment to the privacy of other family members. Nineteen submissions were received which all broadly disapproved of individu-

³⁷ This would also require an amendment to paragraphs (x) and (xi) of the definition of “agency”.

³⁸ Personal Data (Privacy) Ordinance 1995 (Hong Kong), section 52.

³⁹ Data Protection Bill [HL] (UK), 4 June 1998 version, clause 36.



“We consider it very important to ensure that there is a bona fide reason for family members to obtain information about each other and that legal separations should be recognised and give good grounds for refusing access to the other partner’s information.”

- BAYNET CRA LIMITED,
SUBMISSION N12

als being able to rely on the domestic affairs exemption in this way. However, suggestions as to how to address the problem varied. Responses included amending section 56 to prevent the use of this exemption in such circumstances, requiring authorisation for such disclosure, and making this an offence, among other suggestions.

- 6.12.7 This issue is a subset of a wider problem relating to individuals who mislead agencies so as to obtain information to which they are not entitled or to improperly procure the disclosure of information to third parties or the alteration of records. I have proposed in recommendation 148 that a new offence be created relating to the broader issue. However, the issue remains as to how appropriate this exemption is when it is relied upon in such circumstances.
- 6.12.8 I believe it would be desirable to exclude reliance upon this exemption where an individual has misled an agency to release information to which that individual was not entitled. I remain of the view that a number of personal, family and household matters, are best resolved elsewhere than under the Act. I do not want the basic approach to be changed with a series of “domestic squabbles” being brought to the Commissioner. The limits I propose be placed on section 56 will still ensure that only a very precise subset of personal, family or household matters might be the subject of complaint - those involving an individual going outside the family or household to mislead an agency to enable information to be wrongly disclosed. Two other filters should be noted at this stage which should keep the change in proportion:
- the affected individual will need to feel sufficiently aggrieved, and wish to bring an outside agency into the complaint before the matter is handled by my office - many individuals will, even in such situations, wish to deal with the matter directly or within the family or household;
 - to constitute an “interference with the privacy of an individual” there will need to be some sort of harm or detriment of the type outlined in section 66(1)(b).
- 6.12.9 The main problem that has manifested itself is the individual misleading an external agency to obtain information improperly. That is the issue that I propose to address. The breadth of the personal affairs exemption means that other problems also exist, for example:
- an individual pretending to an agency that they are authorised by a family member to request correction or deletion of information or to have it disclosed elsewhere;
 - the individual disclosing the information that has been improperly obtained to further harm the privacy interests of the individual.

However, my proposed change does not seek to tackle those problems since they are not the ones that have primarily manifested themselves in the period under review. Furthermore, if the exemption is lifted too far I have some concern that the law will be drawn into matters which are better attempted to be sorted out within families or households. Accordingly, the changes are solely limited to those in which the individual misleads an agency to obtain information. These are complaints which I presently would investigate because they involve disclosure by an agency in breach of principle 11.

- 6.12.10 Section 56 should be amended so as to make it clear than an individual cannot rely upon the exemption provided for in section 56 where the complaint involves an allegation that the individual has collected personal information from an agency by falsely representing that the individual has the authorisation of the individual concerned, or is the individual concerned. This encompasses principle 1, 2 and 4 complaints. Accordingly, in those complaints the investigation would look at the actions not only of the agency but also of the person who procured the disclosure.

“A significant number of complaints against banks involve inadvertent release of information to third parties, such as former spouses, who have misled the banks in deliberately seeking such information. The Association supports amending section 56 such that persons making deliberate misrepresentations may be held liable.”

- NZ BANKERS' ASSOCIATION,
SUBMISSION N10

- 6.12.11 The tendency would be for the primary scrutiny of the agency to be in relation to principle 5, that is, whether it took reasonable security safeguards, and of the member of the family or household in relation to principles 1, 2 and 4. In reaching a settlement through my complaints processes it would seem appropriate to involve the person who caused the interference with privacy. In a negotiated settlement the person might, for example, offer an apology, undertake not to do the same again, or contribute to any compensation for harm caused. If the matter could not be settled and proceeded to Tribunal proceedings it would be possible for the Tribunal to apportion any compensation to be paid between the agency and the person. At present if such a matter proceeded to the Tribunal the only defendant would be the agency which has been duped into releasing information.



RECOMMENDATION 82

Section 56 should be amended so that an individual cannot rely upon the domestic affairs exemption where that individual has collected personal information from an agency by falsely representing that he or she has the authorisation of the individual concerned or is the individual concerned.

6.13 SECTION 57 - Intelligence organisations

Introduction

- 6.13.1 New Zealand, like other free and democratic societies, has accepted the need for state surveillance to guard against those who would undermine democratic structures. However all democratic societies struggle to find appropriate legal and administrative controls to ensure that any secret services remain accountable to democratic institutions and do not go beyond what is reasonable to achieve their assigned mandate. In New Zealand the limited brief of the former Commissioner of Security Appeals has recently been replaced by an Inspector-General of Intelligence and Security with a wider mandate and greater powers. It is timely to examine the appropriate Privacy Act controls.

- 6.13.2 Secret surveillance and intelligence gathering creates privacy risks for the individuals affected and society at large. To constrain the risks I have taken the view that:

- the role of intelligence organisations should be kept to a tight brief and not be allowed to stray into areas which can be appropriately managed by normal and open governmental and policing activities;
- while the organisations will need to conduct a proportion of their work in secret there will be areas in which some information can be disclosed publicly, to the individuals affected or to oversight bodies, and the greatest degree of openness and disclosure should be promoted;⁴⁰
- as far as possible similar accountability mechanisms as apply to other bodies should apply to the organisations (perhaps in a modified manner) unless there is a good reason for that not to occur; and
- there should be redress for actions of intelligence organisations which breach individual rights without justification, including the right to privacy.

To a significant measure, the laws enacted in 1996 enhance accountability along these lines.⁴¹

Existing position of intelligence organisations

- 6.13.3 Section 57 of the Privacy Act provides:

“Intelligence organisations - Nothing in principles 1 to 5

⁴⁰ For instance vetting is an activity carried out by the NZSIS with the knowledge and assistance of the individual concerned and subject to a complaint appeal procedure. I am also pleased that the NZSIS has taken a further step towards openness, and dispelling misconceptions about the Service's role, by publishing *Security in New Zealand Today*, April 1998.

⁴¹ See Inspector-General of Intelligence and Security Act 1996 and Intelligence and Security Committee Act 1996.

or principles 8 to 11 applies in relation to information collected, obtained, held, used, or disclosed by, or disclosed to, an intelligence organisation.”

- 6.13.4 “Intelligence organisation” is defined in section 2 to mean the New Zealand Security Intelligence Service and the Government Communications Security Bureau (hereafter referred to as the NZSIS and GCSB).
- 6.13.5 Only the principles dealing with access to personal information (principle 6), correction of personal information (principle 7) and unique identifiers (principle 12) at present apply in relation to intelligence organisations.
- 6.13.6 I released a discussion paper which questioned whether the exemption in section 57 should be narrowed so as to apply further information privacy principles to intelligence organisations. I had previously considered the matter in my report to the Minister of Justice on the Intelligence and Security Agencies Bill in February 1996. In the rest of this part of the report I outline the existing position of intelligence organisations under the Act and canvass some of the issues which arise from the proposal to apply information privacy principles 1, 5, 8 and 9 to intelligence organisations.
- 6.13.7 There is a special procedure set out in section 81 for investigations into alleged breaches by an intelligence organisation of principles 6, 7 or 12. Most of the complaints against intelligence organisations received by the Commissioner are against the NZSIS and seek a review of a decision to refuse access to information or to refuse to confirm or deny that it holds any information. The special procedure that applies under section 81 means that neither the Commissioner nor the complainant may refer a complaint to the Complaints Review Tribunal for determination. Rather the procedure anticipates the Commissioner conducting an investigation, forming an opinion, and if the complaint cannot be resolved making a recommendation to the intelligence organisation and awaiting the organisation’s response. If no response is made within a reasonable time or, after considering any comments made by the intelligence organisation, the Commissioner may send a copy of his report and recommendations to the Prime Minister. In turn the Prime Minister may lay a copy of all or part of the report before Parliament. No reports to the Prime Minister have yet been made.
- Extension of other principles to intelligence organisations*
- 6.13.8 There is always a concern in free and democratic societies as to the potentially intrusive intelligence gathering activities of the state. It is not possible for a concerned citizen to know whether such activities, being carried out on his or her behalf, are excessive or are being properly kept in check. The secrecy under which the activities are carried out, the various laws limiting public scrutiny for reasons of national security, and the limited public reporting by oversight bodies, all give rise to anxieties as to whether intelligence organisations are overstepping the mark between prudent intelligence gathering to safeguard society and a more sinister “surveillance state”. The various scandals that surface from time to time with overseas intelligence organisations heighten public concerns.
- 6.13.9 It is desirable that intelligence organisations adhere to the laws that the rest of society lives by, particularly those relating to respect for human rights and accountability to democratic institutions, to the greatest extent possible consistent with the tasks that these agencies are called upon to perform. At the time that the Privacy Act was enacted in 1993 the Government applied information privacy principles 6 and 7 to intelligence organisations (although the special complaints procedure was not as robust or as open as with other agencies). This was a continuation of the access and correction rights which existed under the Official Information Act 1982. However, the Government also applied information privacy principle 12 to intelligence organisations.

VI

“The ACCL has questioned the need for this country to have stand-alone intelligence organisations and in particular the Security Intelligence Service. If there is to be separate intelligence organisations, then in no respect should they be above or exempted from the laws of the land and in particular fundamental human rights laws such as the law protecting individual privacy. We favour the applicability of all of the privacy principles to intelligence organisations.”

- AUCKLAND COUNCIL FOR CIVIL LIBERTIES, SUBMISSION 02

- 6.13.10 It is now the time to apply some of the remaining principles to intelligence organisations (subject to the special investigation procedure which safeguards any reasonable need for secrecy in relation to complaints investigation and determination). I believe that the need is made more urgent by the recent expansion of the mandate of the NZSIS into new areas concerning the security of New Zealand’s economic wellbeing.
- 6.13.11 I take the view that information privacy principles 1, 5, 8 and 9 provide a sound basis for fair information handling and have clear relevance to intelligence organisations. The NZSIS agrees. These principles take account of the purposes of the organisations concerned, apply standards that are reasonable in the circumstances, and would not need to be amended to establish any national security exception.

Principle 1

- 6.13.12 Information privacy principle 1 emphasises the purpose of collection of personal information. In the context of the NZSIS the lawful purpose will be linked to the definition of “security” as set out in the New Zealand Security Intelligence Service Act 1969.
- 6.13.13 I have concluded that principle 1 ought to be applied to intelligence organisations. I am heartened by the fact that no opposition was taken to this proposal (or indeed the ones I suggest below) by either the NZSIS or GCSB.⁴² The NZSIS stated in its submission that:

“Clearly the Service has no authority or wish to collect information that does not meet the criteria in ipp 1 part (a). My interpretation of part (b) is that information is ‘necessary’ if it is required to fully and effectively carry out an organisation’s lawful functions; (ie, if it is evident that it will add nothing in that process then it is not ‘necessary’, but if there is a reasonable expectation that it may, then the requirement of being ‘necessary’ is met). If this view is accepted then ipp 1 presents no concerns to me.”⁴³

- 6.13.14 Both the NZSIS and GCSB made overall comments in relation to the issue in their submissions and made it clear that they did not, for example, necessarily accept the observations made in the discussion paper notwithstanding acceptance of the proposal that additional principles should be applied to the two organisations. GCSB commented that subject to the general observations made, and to “certain caveats” the GCSB would have no difficulty with the proposition that principles 1, 5, 8 and 9 should apply to the Bureau.⁴⁴ The GCSB’s first caveat related to the possible use of the Inspector-General of Intelligence and Security as an appropriate “independent oversight body”. I too believe that it would be valuable to ascribe a role in the context to the Inspector-General and I suggest below that this can be achieved without any change to the statute under which he operates. The GCSB’s second caveat related to principle 9 which is referred to at paragraph 6.13.23.

Principle 5

- 6.13.15 Of all the information privacy principles, principle 5 (storage and security of personal information) would seem to cause least difficulty for intelligence organisations given their emphasis on security of information held and controls on its disclosure. However, in some circumstances there may be information

⁴² Furthermore, all 19 submissions received directly on the point agreed with applying principle 1 to intelligence organisations (see submissions O2-O12, O14-O15, O17, S5, S30, S36, S42 and S52).

⁴³ NZ Security Intelligence Service, submission O14, paragraphs 8 and 9.

⁴⁴ Government Communications Security Bureau, submission S30, page 2.

about an individual which the intelligence organisation has a proper reason to hold but which, through a lapse in reasonable security safeguards or otherwise, is disclosed publicly or to another agency that has no purpose in receiving the information, thereby harming the individual. An example might concern material uncovered in the vetting process.

- 6.13.16 The NZSIS commented in relation to the proposed application of principle 5 to the organisation:

“This principle causes little difficulty for the Service. High standards of physical and personnel security are applied to personal information held by the Service, most of which is both sensitive and classified.”⁴⁵

Nineteen submissions supported applying principle 5 to intelligence organisations.⁴⁶ None were opposed.

Principle 8

- 6.13.17 It might be thought that some small piece of intelligence may seem of little importance at the time it is gathered or shortly thereafter and yet, when accumulated with various other data, achieves a significance weeks, months or years later. However, at the time that the information actually is to be put to use, particularly where a decision based upon it will affect the interests of an individual, it seems reasonable to apply the standards of principle 8, which require that, having regard to the purpose for which the information is proposed to be used, reasonable steps (if any) be taken to ensure the information is accurate, up to date, and so forth. It may be that in the circumstances no checks are feasible and therefore no breach of the principle would be possible. However, where some reasonable step to check information which is to be used in such a way as to affect an individual could be checked this ought to be done.
- 6.13.18 The NZSIS was in agreement with the points made in respect of principle 8 in the discussion paper and offered no objection to the application of the principle to the Service.⁴⁷ Twenty submissions were in favour of applying principle 8 to the intelligence organisations.⁴⁸ None were opposed.

Principle 9

- 6.13.19 If intelligence organisations open files on individuals, which turn out not to be necessary, maintain vast numbers of files on individuals, or retain personal information long beyond when it is properly relevant and useful, there are risks to privacy. Principle 9 would oblige intelligence organisation to have policies on the retention of personal information about individuals so that it is held for no longer than is required for the purposes for which it may lawfully be used. These policies would be linked to the usefulness of the data for an agency’s purposes and, for instance, to the statute under which the NZSIS operates.
- 6.13.20 It would better serve individual privacy if some information was not kept overly long with the dangers that it will paint an inaccurate picture, be out of date, or be misleading. That is not to say that intelligence of a particular nature might nonetheless be held for a long period where it is reasonable to do so. The importance is that intelligence organisations consider the principle and apply it as relevant for their purposes.

- 6.13.21 In respect of principle 9 the NZSIS submitted:

⁴⁵ Submission O14, paragraph 10.

⁴⁶ See submissions O2-O12, O14, O15, O17, S5, S30, S36, S42 and S52.

⁴⁷ Submission O14, paragraph 11.

⁴⁸ See submissions O2-O12, O14, L15, L17, S5, S30, S36, S42, S52 and S54.

“Because of the secrecy of the intelligence agencies, their potential intrusions into New Zealanders lives and the weakness of the oversight and controls on them, it really matters that the Privacy Act is effective. While I think that principles 1, 5, 8 and particularly 9 should indeed be applied to intelligence agencies, and it is hard to see why it mattered to them to want an exemption in the first place, I think the heart of the problem of ensuring reasonable privacy is section 27. The effect of this wording in the Privacy Act is that virtually all information relevant to privacy that is sought from intelligence agencies can be withheld, with the result that privacy principles 6 and 7 appear to be rendered useless.”

- NICKY HAGER, SUBMISSION O8

“What may be considered a reasonable length of time for the retention of information will clearly differ amongst agencies. Intelligence may be gathered in such a way that pieces of information gathered individually and over time in the end present an accurate picture of a security issue. The Service has procedures in place to purge information which is no longer required. It is neither in the Service’s interest nor the public’s to retain outdated information which can serve no relevant purpose any longer. However, it requires a careful judgement to determine when such point is reached in the case of some personal information despite the passage of a substantial period of time since its acquisition.

“Subject to the caveat that security information may need to be retained for a future contingent requirement (eg. an individual may in the future require a security clearance for government employment involving access to classified information) I agree ipp 9 can be extended to the Service.”⁴⁹

- 6.13.22 The GCSB expressed the view in its submission that the intelligence organisation principally concerned with issues relating to the operation of the Privacy Act is the NZSIS. It explained:

“The GCSB is a foreign intelligence organisation and, by definition, our activities have little or no impact on the privacy of New Zealanders.”⁵⁰

- 6.13.23 I am not sure that I agree with that proposition since the privacy principles apply to personal information held by New Zealand agencies whether it is about New Zealanders or foreigners. However, the principal point to note in this regard is that it is not the purpose of the GCSB to engage in gathering information on New Zealanders. This feature came through in the GCSB’s second “caveat” which specifically concerned the possible application of principle 9 to the organisation. Its submission stated that:

“While the Bureau (being, as previously emphasised, a **foreign** intelligence organisation) does not maintain files on New Zealanders, the special nature of the intelligence task does mean that in many cases information acquired and relevant today will still be relevant - perhaps in quite a different context - far into the future. For this reason, it seems to us that, in the application of ipp 9 to the intelligence organisations, there should be some recognition of the special position of information held for intelligence and security purposes.”⁵¹ [emphasis in original]

- 6.13.24 Subject to these caveats the GCSB had expressed the view that it would have no difficulty with the proposition that principle 9 should apply to the Bureau. Nineteen submissions in total supported the application of principle 9 to intelligence organisation⁵² while 1 submission was opposed.⁵³ Two other submissions reserved their position.⁵⁴

⁴⁹ Submission O14, paragraphs 12-13.

⁵⁰ Submission S30, page 2.

⁵¹ Submission S30.

⁵² See submissions O2, O3, L5-O12, L14, L15, S5, S30, S36, S42, S52 and S54.

⁵³ See submission O17.

⁵⁴ See submissions O1 and O16.

**RECOMMENDATION 83**

The exemption for intelligence organisations in section 57 should be narrowed so that principles 1, 5, 8 and 9 apply to information collected, obtained, held, or used, by an intelligence organisation.

Inspector-General of Intelligence and Security

- 6.13.25 I canvassed in the discussion paper whether it would be desirable to provide a role for the Inspector-General of Intelligence and Security in respect of privacy issues. The secret activities of intelligence organisations means that reliance simply upon complaints may be less than satisfactory and the recently created position of Inspector-General seemed to offer a promising oversight agency. Were there to be a suitable role for the Inspector-General it might fall within one or more of the following categories:
- complaints investigation or inquiries;
 - compliance or oversight in respect of information privacy principles relevant to intelligence organisations.
- 6.13.26 In proceeding to consider the appropriate options for the possible involvement of the Inspector-General I have needed to take into account several matters. The first is the statutory scheme of the Privacy Act. For example, I have not seen as compatible with the structure of the Act the devolving of my responsibility of rendering opinions on whether a matter constitutes an “interference with privacy” - although I contemplate that the carrying out of investigations could be a role that is shared through the transfer of complaints. Another is the statutory constraint of the Inspector-General of Intelligence and Security Act 1996. I have presumed that that Act is not to be amended. Third, are the views of the Inspector-General as to the role that may be appropriate for him to play. In that respect, I have been assisted by a submission by the Inspector-General and have taken the opportunity to canvass my proposals with him. There would be little point in proposing a role for the Inspector-General that was seen by the holder of that position as inappropriate.
- 6.13.27 The object of the Inspector-General of Intelligence and Security Act 1996 is, as stated in section 4, to assist the Prime Minister in the oversight and review of the SIS and GCSB. Two particular functions are to ensure that the activities of the agencies comply with the law and the complaints relating to them are independently investigated. The Inspector-General has quite a wide mandate on general inquiry into propriety of particular activities of an intelligence organisation and also has a special function, of interest in a privacy sense, in relation to compliance with the issue and execution of interception warrants. Moreover, the Inspector-General is required to prepare and carry out programmes for the general oversight and review of the two organisations in relation to compliance with the law of New Zealand and the propriety of any of their particular activities.
- 6.13.28 It seems to me that with no further need to amend either statute that there is scope for co-operation, and an appropriate role, for the Inspector-General in relation to privacy matters. For example, in respect of the Inspector-General’s mandate to develop general oversight and review programmes it is possible that checks for compliance with the applicable information privacy principles could easily be built in. In doing this it would be possible for the Inspector-General to consult the Privacy Commissioner on privacy-related matters. No special provision would need to be made in that regard as consultation provisions already exist in both statutes.
- 6.13.29 With respect to investigation of complaints the consultation are also relevant.⁵⁵ In some cases the matter of a complaint could be taken under the provisions of

⁵⁵ See, for example, sections 72B and 117B of the Act.

“We consider it wrong in principle to exempt intelligence organisations from the enforcement mechanisms otherwise provided by the Privacy Act, in particular Complaints Review Tribunal determination (including the availability of damages). The rule of law requires *all* Government agencies to comply with basic human rights such as the right to privacy.”

- AUCKLAND COUNCIL FOR CIVIL LIBERTIES, SUBMISSION 02

the Privacy Act or an Inspector-General inquiry. These provisions help ensure that the complaints are placed with the most appropriate body. Where transfer is not appropriate there can nonetheless be a degree of cooperation to try to ensure that duplication of investigations is minimised.

- 6.13.30 The compliance programmes that the Inspector-General is empowered to carry out hold particular promise for certain of the privacy principles that I recommend be applied to intelligence organisations. Indeed, compliance programmes will be a far more suitable way of achieving benefits for privacy than simply awaiting complaints. For example, it will be more satisfactory for retention issues under principle 9 to be gone into as part of a compliance programme, than simply to await an individual to lodge a complaint alleging that information about him or her has been retained where there is no lawful use for that information.

Part VII

VII

Public Register Personal Information

231

“Public bodies should be able to avoid the communication to third parties of personal data which is stored in a file accessible to the public and which concern data subjects whose security and privacy are particularly threatened.”

- Council of Europe, *Recommendations on Communications to Third Parties of Personal Data held by Public Bodies*, 1991

“Drawing general principles is a challenging task. Precedents can be found from one extreme to the other. Some records are entirely public and available for use without restriction. Some records are not available to the public under any circumstances. There are a variety of intermediate models that illustrate partly open or partly confidential disclosure systems, with either statutory, regulatory, or wholly discretionary standards.”

- Robert Gellman, *Public Records: Access, Privacy, and Public Policy*, 1995.

“The newspaper industry recognises that there are significant issues of practicality and individual safety which arise from the publication and availability of public registers. Nevertheless, we firmly believe that the general rule should be that a public register is just that - public - and that inappropriate use of any register is solved in other ways.”

- Commonwealth Press Union, submission T8

“No matter what work is done to make the PRPPs adequate, they still rely to a large extent on the legislation establishing the public register.”

- Franklin District Council, submission T2

7.1 INTRODUCTION

Overview

- 7.1.1 Part VII concerns public register personal information. It includes sections 58 to 65 of the Act and links to the Second Schedule which sets out the public registers covered. After looking at some aspects of terminology, this part of the report surveys public register issues and risks and notes aspects of consultation on the issue. The report then moves to a section by section commentary and analysis with recommendations as appropriate.

Terminology

7.1.2 This part of the report is concerned with the privacy issues surrounding registers of personal information maintained by public authorities. Registers are essentially formal records set down in a systematic way for use and retrieval. The registers that this paper is particularly interested in are those to which the public has been given a right of search, such as:

- the register of land titles held at the Land Transfer Office;
- the register of motor vehicles maintained by the Land Transport Safety Authority on behalf of the Ministry of Transport.

7.1.3 Since they are usually maintained by public authorities under the authority of an enactment, registers will be referred to in this part of the report as “statutory registers”. Most of the discussion will focus upon those statutory registers for which a special right of public search is granted in the relevant enactment.

7.1.4 The Privacy Act has identified certain statutory registers which are open to search and applied special controls to them. The statutory registers maintained under the enactments listed in the Second Schedule to the Privacy Act are referred to as “public registers”. Note that “public register” therefore has a special technical meaning in the Act and does not refer to all statutory registers open to public search.

Council of Europe Recommendation R(91)10

7.1.5 Although the Council of Europe Convention No 108 generally makes no distinction between the protection of personal information in the public and private sectors, it has issued recommendations which are specific to “personal data held by public bodies”.¹ In general terms this equates to information on public registers. Parliament has directed me in section 13(1)(e) to have regard to the Council of Europe Recommendations on Communications to Third Parties of Personal Data held by Public Bodies when reviewing the public register privacy principles. I quote an extract from the preamble:

“Noting that automatic data processing has enabled public bodies to store on electronic files the data, including personal data, which they collect for the purposes of discharging their functions;

Aware of the fact that new automated techniques for the storage of such data greatly facilitate third party access to them, thus contributing to the great circulation of information within society ...

Believing however that automation of data collected and stored by public bodies makes it necessary to address its impact on personal data ... which are collected and stored by public bodies for the discharge of their functions;

Noting in particular that the automation of personal data of personal files has increased the risk of infringement of privacy since it allows greater access by telematic means to personal data ... held by public bodies as well as communication of such data ... to third parties;

Mindful in this regard of the increasing tendencies on the part of the private sector to exploit for commercial advantage the personal data ... held by public bodies as well as the emergence of policies within public bodies envisaging communication by electronic means of personal data ... to third parties on a commercial basis;

Determined therefore to promote data protection princi-

¹ Council of Europe, Recommendations on Communication to Third Parties of Personal Data held by Public Bodies, R(91)10, 1991 (hereafter referred to as Recommendation R(91)10).

ples based on the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data to ensure that the communication by public bodies of personal data ... to third parties, in particular by electronic means, has its basis in law and is accompanied by safeguards for the data subject;

Noting in particular that these data protection principles should be reflected in the new automated context which now characterises the communication of personal data ... to third parties under legal provisions governing accessibility by third parties to personal data ...”

I will make further reference to Recommendation R(91)10 below, especially in relation to public register privacy principles 1, 2 and 3.

Public register issues and risks

- 7.1.6 Public registers have particular characteristics which carry special privacy risks and raise difficulties in legally and practically addressing those risks in an effective fashion.
- 7.1.7 In considering the privacy risks one should bear in mind the following characteristics of a typical public register:
- the information on the register will be logically arranged to enhance analysis, use and retrieval of the data - while this is essential to the proper functioning of the register for its necessary purposes, it also makes it an especially attractive source of information for other purposes;
 - only key authoritative data is registered - unlike many other structural record systems (such as government files) a statutory register is unlikely to be cluttered with extraneous material such as draft documents or correspondence, making it straightforward to quickly locate relevant information;
 - the existence of the register will be well known - making an easier source for third parties searching for data;
 - the register will have a degree of institutional permanence - which may enable third parties to plan elaborate and ongoing processing of the data for unrelated purposes;
 - individuals will be compelled by law to supply personal information for the register or else they will commit an offence or be unable to undertake some activity - this compounds the affront to privacy when information is used for unrelated purposes;
 - certain sets of information exist only in public registers since individuals are unwilling to provide the information voluntarily;
 - a statutory right to search the register exists which restricts a registrar’s discretion to withhold information.
- 7.1.8 Accordingly, many public registers are attractive propositions for all sorts of third parties who would wish to use them to obtain information about individuals - indeed, some businesses specifically “mine” public registers and sell the results. Briefly stated, the central privacy issues with public registers revolve around the fact that individuals have no choice but to supply their public details which may then be published and will be given out on request to whoever wishes to have the information without regard to the purpose for which that information will be used or the harm that any such use may cause an individual.
- 7.1.9 Typical public register privacy problems are:
- their use for tracing individuals for reasons unconnected with the purpose for which the register was established, whether those reasons be relatively benign (preparing a family history) or malign (tracking an estranged partner who has fled from an abusive relationship);

“Council does receive complaints from time-to-time from members of the public regarding the use of public register information by direct marketing companies and the like.”

- TAURANGA DISTRICT COUNCIL,
SUBMISSION T7

- bulk retrieval of personal information on public registers by commercial interests which use and sell the information for direct marketing purposes or for profiling individuals (for instance, as to their wealth or creditworthiness).

7.1.10 The nature of public registers also creates difficulties in tackling the privacy problems effectively. Some of these difficulties include:

- the fact that many statutory provisions give little explicit guidance as to the purpose for which a register was established;
- few statutory provisions establishing registers themselves attempt to address any privacy issues;²
- the evolution from traditional paper-based, and office-bound, registration systems to automated systems, with potential for on-line searching, removes previous privacy protection which incidentally existed through physical constraints and inefficiencies and the need for human intervention;
- the interaction between two pieces of legislation, the Privacy Act and the public register privacy provision;³
- the compulsory, or non-voluntary nature of the registers, restricting the use of authorisations, or opt-in/opt-out provisions which are often a suitable mechanism for resolving privacy problems in other contexts;⁴
- the lack of data protection “infrastructure”, such as audit mechanisms, rules out some otherwise feasible privacy solutions.

Consultation

7.1.11 Since 1993 significant thought has been given to public register privacy issues. I have, for example, encouraged discussion of the issue at the annual Privacy Issues Forum. Papers prepared for these conferences included in 1994, 1995 and 1997:

- Public registers - A discussion paper;
- Public register privacy issues - some issues for local government;
- Public registers and profiling;
- Public registers and personal safety;
- Public registers - recent developments and what’s wrong with the public register privacy principles.

7.1.12 To further inform discussion about public register issues, and promote compliance with the public register privacy principles, my office released in 1997 a compilation of materials on the subject.⁵ From my 1995/96 annual report onwards I have reported on public register issues in a separate part of my annual report. I have also been active in scrutinising, and reporting to you in relation to, proposed legislation bearing upon the statutory registers open to public search.

² Sometimes bodies maintaining statutory registers make decisions to protect privacy within the bounds of their statutory powers. For example, a registrar might choose not to place residential addresses on a public register notwithstanding that the statute is silent on the matter. However, what I am noting here is that very few statutory provisions themselves seek to address privacy issues. The few that do usually permit an individual to apply to have their details treated in a special way. Such provisions usually turn upon some objective grounds rather than a desire for privacy. For example, an elector is permitted to have details withheld for personal safety from the published electoral roll. Under the Building Act 1991, plans to be placed on a building consent register can be marked “confidential” by owners for reasons of security or copyright.

³ With the Domestic Violence Act 1995 as a further player and, on occasion, the Official Information Act 1982 or the Local Government Official Information and Meetings Act 1987, making a showing.

⁴ However, the Radiocommunications Amendment Bill, presently before Parliament, attempts in an innovative way to address the matter through the inclusion of an “opt-in” arrangement whereby address details will not be released except with the authorisation of the individual (since in that instance the disclosure of address details is not required for any official or necessary purpose of the register but registered individuals may find it personally beneficial to have their details released to associations of radiotransmitters). See Report of the Privacy Commissioner to the Minister of Justice in relation to the Radiocommunications Amendment Bill, 19 January 1998.

⁵ A Compilation of New Zealand Materials in Relation to Public Register Privacy Issues, January 1997.

- 7.1.13 As part of the consultation on this review I released a 28-page discussion paper in September 1997. Thirty-one submissions were received. A consultation meeting held with representatives from a variety of Wellington region local authorities was held in Wellington in December 1997. Although the meeting canvassed other local authority issues the main focus of discussion was public register issues.

SECTION BY SECTION DISCUSSION

7.2 SECTION 58 - Interpretation

- 7.2.1 Section 58 defines three terms specifically for Part VII. None of the definitions has given difficulty in operation. Issues I will canvass are:
- whether it would make the Act more “user friendly” if the definitions were located in the general interpretation provision, section 2;
 - whether there is a case to extend the meaning of “public register” to include all statutory registers open to search; and
 - whether there is a case for further definitions.

Location of definitions

- 7.2.2 Section 58 defines three terms: public register, public register privacy principle and public register provision. Each of these is principally, but not exclusively, to be found in Part VII. For example, “public register” is also to be found within the definition of “publicly available publication” which is used in Parts I and II. “Public register privacy principle” is found also in both Parts II and VIII.

- 7.2.3 Both “public register” and “public register privacy principle” are defined in section 2. In each case, the relevant definitions simply say that the term “has the meaning given to it in section 58”. I do not believe that the operation of the Act would be enhanced by moving the section 58 definitions into section 2.

Definition of “public register”

- 7.2.4 The term “public register” is currently defined to mean:
- (a) any register, roll, list, or other document maintained pursuant to a public register provision; or
 - (b) a document specified in Part II of the Second Schedule.
- The list of public register provisions is set out in the Second Schedule to the Act and Appendix I of this report.

- 7.2.5 Accordingly, a statutory register open to public search will only become a “public register” in terms of the definition when it has been suitably identified in the Second Schedule. It follows that there may well be a number of registers, rolls, lists or other documents maintained pursuant to enactments which have similar characteristics to the existing “public registers”. Indeed, that is clearly the case.⁶ Although the list in the Second Schedule captures many of the more important registers it is by no means comprehensive. Aspects of this issue have already been canvassed in the preceding introductory section of this part of the report and I will return to it in relation to section 65.⁷

- 7.2.6 A suggestion, made in several submissions, is that “public register” be redefined to include all statutory registers open to public search rather than just those listed in the schedule.

- 7.2.7 A suitable definition might be:

⁶ Discussion paper No. 5 listed some 50 statutes understood to contain provisions establishing statutory registers which are not “public registers”.

⁷ See paragraph 7.14.

Public register means any register, roll, list or similar document:

- (a) maintained pursuant to a provision contained in an enactment; and
- (b) which is required to be open to public search pursuant to a provision in that enactment.

- 7.2.8 The elements of such a definition indicate:
- that the register must have a register-like form - that is, being a register, roll, list or other similar document;
 - that it be maintained pursuant to a provision in an enactment - that is having a “public” and official character being maintained under law;
 - be open to search - that is having a “public” character in the sense of the information on the register being accessible to the public;
 - that it be a legal right of access - that is, that the register be required to be open to search by law rather than for its openness to be a matter of administrative discretion and to distinguish a register from the more general availability of official information under the Official Information Act.⁸
- 7.2.9 If such a definition were to be adopted it would be possible to dispense with the Second Schedule and the specific listing of public registers. It would be possible to modify the definition so that a “public register” includes those maintained pursuant to a public register provision set out in the schedule *and* any other register of the type coming within the general definition.
- 7.2.10 In my view, it would be possible for the regime to work suitably in relation to a general definition to be drafted. The fact that the public register controls defer to other enactments will mean that significant operational problems would be unlikely to be encountered.
- 7.2.11 However, I recommend continuing with the present definition and to couple this with a systematic effort to identify registers having the characteristics of “public registers” and add them to the Second Schedule. It seems to me that the making of a conscious decision to add an entry to the list of public register provisions is a valuable one. It retains certain advantages over the adoption of a general definition, including:
- the effect of the extension of public register controls to a wider range of registers will be better understood;
 - certainty with respect to the scope of any extension of the regime;
 - the resultant schedule will provide a picture of the series of registers to which the regime applies and this transparency or openness is a desirable objective of data protection laws;
 - the effect of disclosure under principle 11 will be clearer;
 - the agencies which administer the registers will better understand their responsibilities if they have participated in identifying the relevant provisions and have been consulted on the application of the regime to them;

⁸ Obtaining information from a register pursuant to a statutory search right differs in nature from an Official Information Act request. In an Official Information Act request, the requester sets the parameters through the scope of the request. A register search, on the other hand, does not usually have this individualised quality. Requests for information from a register must fit the requirements of the agency maintaining the register and not the other way round. A request under the Official Information Act requires an official to consider whether there are grounds for withholding the information. Judgment and discretion are called for, and occasionally consultation. The official may withhold information although before doing so will consider any countervailing public interest favouring disclosure. A request for information from a public register is far more mechanistic. If the registrar’s requirements are met, such as through the use of a search form or the payment of a fee, the information in standardised form will be released, usually quite promptly. The Official Information Act does not derogate from provisions in enactments which authorise or require official information to be made available. Statutory search rights concerning registers are such provisions.

- there seems to be little privacy “downside” in the delay inherent in systematically bringing further registers into the regime - the information on the registers remains subject to the information privacy principles;
- the opportunity for Parliament to define the purposes of a register as it takes the decision to add a provision to the schedule.

Possible new definitions

7.2.12 In the discussion paper on this Part of the Act I sought views upon whether certain terms used in Part VII should be defined. I also asked whether any other terms should be defined. Amongst the terms considered were “re-sorted” and “combined”, used in public register privacy principle 2, and “electronic transmission” and “member of the public”, used in principle 3. At this point I simply observe that in my view it is not necessary to provide further statutory definitions at this time.

7.3 SECTION 59 - Public register privacy principles

7.3.1 Section 59 establishes the four public register privacy principles. They cover the following topics:

- principle 1 - search references;
- principle 2 - use of information from public registers;
- principle 3 - electronic transmission of personal information from registers;
- principle 4 - charging for access to public register.

There follows a discussion of each principle with suggestions for two further principles.

7.4 PRINCIPLE 1 - Search references

7.4.1 Public register privacy principle 1 states:

PRINCIPLE 1

Search references

Personal information shall be made available from a public register only by search references that are consistent with the manner in which the register is indexed or organised.

7.4.2 The term “search reference” is not defined but the meaning seems clear. It refers to the information that must be cited by the public when seeking to obtain information from a register. Typical search references include:

- name;
- address;
- licence or document number.

7.4.3 Search references have traditionally relied upon the way in which a register is organised. For example, if certificates of naturalisation are stored in filing cabinets in date order depending upon the day on which citizenship is granted it is likely that the search references would be sequential document number, date of citizenship, or for a broader search, year of citizenship. Retrieval based on a person’s name would not be possible.⁹ Conversely, if the register was organised alphabetically by surname of new citizen it would not be possible to search solely by document number or date of citizenship. To compensate for the physical limits on easy retrieval of data, registrars would typically prepare an index to enable ready retrieval by other appropriate search references.

7.4.4 The principle makes it clear that the agency maintaining the register can only allow the information to be made available by search references which meet the principle’s criteria. Looked at from the other side of the counter, a person

⁹ Although typically an *index* by name would also be prepared to allow for such retrieval.

searching the register could not insist on having access to information by citing some other reference (in the example given, by citing country of origin).

Search references and purpose of a register

7.4.5 When legislation establishes a new register, officials have the task of devising suitable administrative arrangements. At the point of establishing the register officials are keenly aware of the purpose for which it has been established and fully understand the need for the relevant information to be retrievable for the appropriate purposes. For example, in establishing a register of motor vehicles it will be known that the information will need to be retrieved by licence plate number whereas there may be little need to retrieve information by reference to other information held, such as vehicle colour. If there is no legitimate need to search such a register by individual's name it is unlikely that the search reference will be built in to the way that register is indexed or organised.

7.4.6 The brevity and simplicity of the principle belies its importance. Search reference limits often act as an effective privacy protection device. By prohibiting the addition of search references inconsistent with the manner in which the register is indexed or organised there is thereby a privacy protection. For example, a search by owner's name using the vehicle register would effectively create a national locator of persons, something that would not have been the subject of debate in creating the register.

7.4.7 Notwithstanding the preceding discussion, it does not always follow that existing search references will mirror the purposes for which a public register has been established and public search rights granted. Reference to "the manner in which the register is indexed or organised" is an imperfect way of seeking to ensure that the search references enable access to the personal information held consistently with the purpose for which the register was established. Strictly speaking the most the principle would achieve is that the registrar "calls the shots" in that the member of the public cannot insist on search references which differ from those inherent in the register's organisation or contained in the agency's index. Although, as suggested, the existing principle should ensure some correlation with the purposes underlying the register, this is not explicit and will not be borne out in some cases (for example, if a very broad index, with many search categories, had been created).

7.4.8 Furthermore, the computerisation of such records, together with advances in the flexibility of computer database programs, means that items of information can be accessed and sorted in countless ways without obvious effort. In such computer systems some would argue that it is perhaps no longer meaningful to think of the register being "indexed or organised" by some limited set of search references. For those systems - and *a fortiori* for the next generation of database technology - the existing principle 1 may be simply ineffective.

7.4.9 I examined the possibility of incorporating within the principle an express reference to a register's "purpose". In the relevant discussion paper I proposed that the principle be amended to read:

Personal information shall be made available from a public register only by search references that are consistent with the manner in which the register is indexed or organised *and with the purpose of the register.* [change highlighted]

7.4.10 Most submissions supported the proposed change seeing it is as an appropriate way to tackle the privacy issues.¹⁰ Particularly notable was the strong support

¹⁰ Sixteen out of 18 submissions agreed that principle 1 should require search references to be consistent with the purpose of a register - see submissions T1, T9, T11-T15, S27, S36, S42, S51 and S58. One submission opposed the proposition (T10) while submission T17 considered that this was already required under the current principle.

“You may be aware of this Council’s prolonged challenge regarding the ability of organisations to access personal information from the building consent register. The outcome favoured releasing the information. It is frustrating, therefore, that such an outcome would seem to totally contravene the spirit of the Privacy Act. Irrespective of the prevailing legislation, this Council firmly believed that more weight should have been given to the purpose of the collection of the information and its commercial value. Suffice to say, that along with probably every other local authority in New Zealand we are now selling on a cost recovery basis, building consent information to organisations which intrude upon the privacy of individuals to use it for commercial gain.”

shown in local government submissions. The limited opposition in the submissions came not from the agencies which maintain public registers (although some practical issues were raised in the submissions, particularly over the process for “fixing” purpose) nor from agencies representing or having a role in relation to persons whose personal information is displayed on public registers. The main submission in opposition was by a credit reporting agency (submission T10).

- 7.4.11 I have concluded that the proposed change to principle 1 would be a desirable amendment to enhance privacy and the appropriate functioning of the public register privacy principles. A reference to purpose will make the principle more understandable to anyone familiar with notions of information privacy and will directly address shortcomings in the present principle. The resultant principle will, in my opinion, be workable.



RECOMMENDATION 84

Public register privacy principle 1 should be amended so that search references be required to be consistent with the purpose of a particular register.

Establishing purpose of a register

- 7.4.12 Given my recommendation that search references be consistent with purpose, it is necessary to consider how “purpose” is to be ascertained. I have already noted that public register provisions frequently give little explicit guidance as to the purpose for which a register was established. For that reason, I canvassed in the discussion paper whether it would be desirable to establish a particular mechanism for defining a register’s purpose. If a mechanism were to be crafted there would be several issues to address:
- who would be the decision maker in fixing purpose? Candidates would include the relevant department, Minister, the Executive Council (through regulations), Parliament (through statutes) or the Privacy Commissioner (through code of practice or a new mechanism).
 - What process would be followed? For instance, would the Privacy Commissioner or public have to be consulted? Would the resultant statement be published in the Gazette?
 - What legal status would a statement of purpose have in the event of a complaint? If the purpose was established under an enactment, such as within a public register provision or in statutory regulations, this would prevail by reason of sections 7 and 60 of the Privacy Act. Similarly, if the Commissioner established statements of purpose pursuant to a code of practice, the Act would give them an automatic status.

- 7.4.13 On the subject of “purpose”, clause 4.1 of Recommendation R(91)10 states:

“The purposes for which the data will be collected and processed in files accessible to third parties as well as the public interest justifying their being made accessible should be indicated in accordance with domestic law and practice.”

- 7.4.14 For several years my office has suggested to departments which enact or re-enact public register provisions that they include a statement of any register’s purpose. As a result, for example:
- Local Government Act 1974, section 122ZI, provides that the register of charges established under that section is “for the purposes of enabling any member of the public to establish, verify, or assess the charges registered against the asset or assets of a local authority and the nature and terms of the obligations that those charges secure”;
 - Radiocommunications Amendment Bill, clauses 3 and 11, specifies that the registrar must maintain a register “for the purposes of maintaining records of interests or uses relating to radio frequencies” and that any person may

“The many statutes that require, permit, or prohibit the disclosure of specific categories of public records would appear to offer a wealth of material from which more general principles can be deduced and policies can be isolated. In practice, this is much more difficult than it appears. For many statutes, it is not possible to find materials explaining [why] the law was written in a particular way. Even if materials may be found, they may not reflect current controversies.”

- ROBERT GELLMAN, *PUBLIC RECORDS: ACCESS, PRIVACY, AND PUBLIC POLICY*, 1995

have access “for the purpose of determining whether or not any radio frequency is subject to a record of management rights, a spectrum licence, or a radio licence, and determining the identity of the owner of a management right, a right holder, or the holder of a radio licence.”

- 7.4.15 Statutory statements of purpose remain rare. Whether or not public register privacy principle 1 is amended, I believe that it continues to be desirable for new statutory registers to have that purpose explicitly stated. Statutory statements of purpose will guide the agencies administering the register as well as the users of registers and the Privacy Commissioner in investigating complaints. Any *statutory* statement of purpose will have priority in any scheme devised since it will take precedence over regulations, codes of practice or administrative decisions.
- 7.4.16 Given that few statutes currently contain statements of purpose, it is necessary to consider whether:
- all public register provisions should be amended to contain a statement of purpose;
 - an alternative mechanism for fixing statements of purpose is desirable; or
 - an amended principle 1 can operate satisfactorily without any new mechanism to fix purpose being created.
- 7.4.17 I have concluded that it would not be desirable to seek to amend, in one hit, every public register provision so as to include a statement of purpose. This would require a commitment of resources by departments and my office which is not warranted as a priority. Rather, I am content with pursuing the merits of that approach on a register by register basis as opportunities arise for review, amendment or consolidation.



RECOMMENDATION 85

As new public register provisions are enacted, or existing ones reviewed or consolidated or amended, consideration should be given to including statutory statements of purpose.

- 7.4.18 It is possible to devise a new mechanism, to be located within Part VII of the Privacy Act allowing for a statement of purpose to be fixed. Such mechanisms could include the following options:
- a power enabling regulations to be made in respect of any public register provision stating the purposes for which a public register is established and made available for public search;¹¹
 - a mechanism for the Minister or agency which maintains a public register to produce a draft statement of purposes, to notify this, undertake public consultation, and then issue a final statement by Gazette notice which has effect until revised following a similar process;
 - a Privacy Commissioner-initiated process involving the release of a proposed statement, public consultation, and issue which would be subject to Parliamentary disallowance, modelled upon, or forming part of, code of practice provisions;
 - a statutory requirement for departments to produce and have available for the public on request a statement of purposes.
- 7.4.19 Any of these alternatives is, in my view, workable. The merit in any one depends upon whether one believes such decisions should be taken at the Parliamentary, Governmental, or administrative level or by an independent Commissioner. There are also considerations of competing calls for resources, such as in relation to Parliamentary time.

¹¹ A single set of regulations is likely to be impractical. It is anticipated that regulations would be developed only as needed and perhaps included within any general sets of regulations concerning a register.

- 7.4.20 My view is that where a bill is before the House these decisions should be taken by Parliament. However, I do not characterise the issue as one that ought to demand Parliamentary attention in the absence of new, amending, or consolidating, legislation coming before the House. I believe that the devising of suitable statements of purposes are well within the capabilities of departments. As the stewards of the information, and as the people most familiar with their own legislation, departments should have initial responsibility for preparing any statements of purpose. Any process followed should involve proper consultation outside the department.
- 7.4.21 However, as a supplement to any administrative process initiated by departments, it may be useful to allow for the issue of regulations to specify purposes. Such regulations should be made after consultation with the Privacy Commissioner. It would be unnecessary to issue such regulations in respect of all public registers. However, the option would be there in the event that it is desired to obtain greater transparency in respect of a particular register. Regulations would provide an alternative to seeking a code of practice from the Privacy Commissioner and a “fast-track” alternative to obtaining amendment legislation. Accordingly, consideration could be given to placing a general regulation-making power in the Privacy Act.

**RECOMMENDATION 86**

Consideration should be given to establishing in the Act a regulation-making power to specify, in respect of any particular public register, the purposes for which the register is established and is open to search by the public.

- 7.4.22 The position for registers not having a statement of purpose in statute, regulation or code will be similar to that of practically all agencies in relation to their holding of any personal information. New Zealand does not operate a register of all permitted uses or purposes as do European countries. Judgments have to be made all the time as to what is a “purpose connected with a function or activity of an agency” or is a purpose for which information is collected or obtained (information privacy principles 2, 3, 9, 10 and 11). Even in the absence of a complaint, agencies must be ready to tell individuals the relevant purposes or to answer my queries under section 22 if necessary.
- 7.4.23 Formal public register complaints are not common at present and I have no particular reason, absent controversial decisions by departments to extend search references beyond the reasonable bounds of their statutory mandate, to think that this will change significantly in the future. If a complaint is received I will, as with other complaints, receive representations from the agency and complainant and will, if necessary, form an opinion as to the relevant issues. In the event of disagreement with the department I will, on the present complaints processes, provide a recommendation to the relevant department or Minister.¹²

7.5 PRINCIPLE 2 - Use of information from register

- 7.5.1 Public register privacy principle 2 states:

*PRINCIPLE 2**Use of information from public registers*

Personal information obtained from a public register shall not be re-sorted, or combined with personal information obtained from any other public register, for the purpose of making available for valuable consideration personal information assembled in a form in which that personal information could not be obtained directly from the register.

¹² Privacy Act, section 61. Elsewhere I recommend that public register complaints be fully enforceable and be able to be taken to the Tribunal (see paragraph 7.10.5 and recommendation 95). In such an event it will be possible for a ruling of the Tribunal to be obtained.

“The Council agrees that public registers (not merely those restricted to local authorities) are often used for reasons unconnected to the purpose for which the registers were established.”

- PALMERSTON NORTH CITY
COUNCIL, SUBMISSION T4

Council of Europe Recommendation R(91)10

7.5.2 Clause 7 of Recommendation R(91)10 states:

“Unless permitted by domestic law providing appropriate safeguards, the inter-connection - in particular by means of connecting, merging or downloading - of personal data files consisting of personal data originating from files accessible to third parties with a view to producing new files, as well as the matching or interconnection of files of personal data held by third parties with one or more files held by public bodies so as to enrich the existing files or data, should be prohibited.”

Application to every person

7.5.3 While all four of the principles apply to agencies responsible for administering a public register, principle 2 also applies to every other person.¹³ The principle does not simply guide the actions of registrars - it also constrains the use of information obtained from public registers by other persons. The principle attempts to address the risks of information which is supplied compulsorily for public registers being reprocessed for other purposes without the approval of the individuals concerned. However, unlike the Council of Europe Recommendation R(91)10, principle 2 only prohibits such activities if they are carried out for the purpose of on-selling the enriched information.

7.5.4 The principle is also necessary so as to ensure that the other principles are not undermined. For example, consider a register which does not utilise the name of the individual as a search reference. Principle 1 would be undermined if a company can obtain all the information from the register and makes it available electronically through different search references. It is the same information that was obtained compulsorily and the same privacy risks arise.

7.5.5 In recommendation 95 I propose that the public register privacy principles become enforceable in a similar manner to the information privacy principles. This would enable complaints against the agencies maintaining public registers to be taken right through to the Tribunal if necessary. The proposal is also that complaints against any other agency which breached principle 2 be able to be taken to the Tribunal. I will not further repeat those recommendations here.

Layout

7.5.6 While I do not recommend any substantive amendments to principle 2 at this stage I do consider that it would benefit from a slight drafting change.

7.5.7 The principle has several elements within it which are expressed either as alternatives or as cumulative requirements. Although these elements are relatively straightforward if one takes care to consider the principle, the task is not made as easy as it might be through its layout as a single lengthy sentence. I suggest that the elements expressed as alternatives near the start of the principle be separately stated as itemised paragraphs. Accordingly, the reformed principle would read as follows:

Use of information from public registers

Personal information obtained from a public register must not be:

(c) re-sorted; or

(d) combined with personal information from any other public register:

for the purpose of making available for valuable considera-

¹³ Refer section 60(2). See also my proposal to amend that section in recommendation 94.

tion personal information assembled in a form in which that personal information could not be obtained directly from the register.

**RECOMMENDATION 87**

Public register privacy principle 2 should be re-enacted with a structure which more clearly leads users to identify its elements.

7.6 **PRINCIPLE 3 - Electronic transmission of personal information from public register**

7.6.1 Public register privacy principle 3 states:

PRINCIPLE 3

*Electronic transmission of personal information
from public register*

Personal information in a public register shall not be made available by means of electronic transmission, unless the purpose of the transmission is to make the information available to a member of the public who wishes to search the register.

Manual to computerised registers

7.6.2 This principle tackles the means by which information is increasingly made available from public registers. Traditionally registers were paper based and often consisted of files in filing cabinets or entries written in a book. Getting access to a register meant one had to visit the public office, ask to see the entry, and to have this brought to the desk for perusal. Later, with the advent of photocopiers, it became usual administrative practice, sometimes reflected in statutes, for access to be given by photocopying an extract from the register. Extracts could be made at the public office, or requested in writing, usually on payment of a copying fee. With the advent of computers, entries could be given by computer printout.

7.6.3 Until quite recently, few public registers have been completely computerised. This is becoming more usual now.¹⁴ Computerisation of the registers is becoming increasingly sophisticated. Information can be supplied on computer disk for entry on some registers. Searches on some registers can already be made on-line.

7.6.4 The principle attempts to place a brake upon making information available from public registers generally by means of electronic transmission. “Electronic transmission” encompasses, amongst other things, downloading information to disk or tape for reading by another computer as well as on-line transmission. The exceptions where electronic transmission is permitted include:

- where the purpose of the transmission is to make the information available to a member of the public who wishes to search the register - principle 3 itself;
- where a statute authorises the action - section 60(3); or
- where a code of practice authorises the action - section 64(a).

Privacy risks of electronic transmission

7.6.5 There are a variety of privacy risks associated with electronic public registers since information can be extracted and used or manipulated with ease compared with non-electronic data. For example, in electronic form:

- thousands of records can be matched against others within fractions of a second;

¹⁴ Although sometimes a “computerised” register simply mirrors paper records which comprise the legally authoritative version for certain official purposes.

- data can be added to other records with ease creating new databanks and enabling the profiling of individuals;
- sophisticated and unexpected searches can be made with ease (for example, a search of “red BMW cars owned by women living in Seatoun” is feasible electronically but not with manual records);
- errors in records can be rapidly transmitted to other databases and the effects on individuals multiplied;
- registers may be vulnerable to remote access (“hacking”) with attendant risks of disclosure, loss or alteration of data;
- electronic transmission of data may enable persons to construct a full copy or substantial extract from a public register which could then be re-worked so as to be put to different private uses.

7.6.6 This is just a selection of risks. It is not comprehensive. Nor should it be taken as an argument against computerising public registers. Good public administration precludes any suggestion that public registers be “off limits” and maintained with yesterday’s technology. However, given the nature of public registers, including the compulsion by which information is obtained and the right to public search, the implications of moving from manual to computerised processing should not be overlooked. The point at which the register interfaces with the outside world (the point of transmission or search) is a key aspect of controlling the risk.

7.6.7 The extracts from the preamble to the Council of Europe recommendations, quoted at paragraph 7.1.5, give a “flavour” of the international concern about electronic transmission of information from registers. While the Privacy Act generally takes a “technology neutral” view of the processing of information Recommendation R(91)10 supports the case for special controls relating to the electronic transmission of personal information.

7.6.8 Principle 3 can be criticised for not going as far as the Council of Europe Recommendations. For example, clause 5.2 of the Recommendations says:

“At the time of automatic communication, technical means designed to limit the scope of electronic interrogations or searches should be introduced with a view to preventing unauthorised downloading or consultation of personal data or files containing such data.”¹⁵

7.6.9 Indeed principle 3 might be seen in some respects as permissive rather than restrictive. Some agencies maintaining statutory registers seem to take an “all or nothing” approach and suggest that once the information is made available electronically it is no longer feasible for the agency maintaining the register to attempt to protect privacy interests or to control the purpose for which people using the register are searching it. This is typically the response of agencies which, perhaps without much study of the implications from a privacy perspective, make records directly available on the Internet. Sometimes such records are placed with minimal controls or controls which are easily circumvented for commercial or other purposes. I believe that there is technology available which can automatically search holdings of information on the Internet thereby enabling a vast amount of data to be downloaded to create a duplicate database searchable by whatever references the new possessor of the data chooses.¹⁶

7.6.10 Paragraph 5.2 of the Council of Europe Recommendation R(91)10 suggests that agencies should continue to recognise their responsibilities when design-

¹⁵ However, information privacy principle 5 does envisage security safeguards being taken.

¹⁶ Some of the risks have recently been canvassed in the Common Position of the International Working Group on Data Protection in Telecommunications, “Data Protection and Search Engines on the Internet”, 15 April 1998.

ing facilities to make information available electronically. For example, attention should be paid to the technical means which may be available to continue to protect the data. Where these are clearly inadequate, it is questionable whether the information should be made available electronically at all. This is especially the case with information that has been obtained compulsorily from individuals. The approach of Recommendation R(91)10 is that such information should not be made available to third parties without individual authorisation.¹⁷ Where the storage of the personal information in a file accessible to third parties is not obligatory, clause 6.2 of Recommendation R(91)10 recommends that the individual be made aware of the proposed accessibility of the information and advised of the right to have the personal information stored in a way that is inaccessible to third parties.

7.6.11 In terms of the electronic transmission of personal data held by public bodies, the Recommendation R(91)10 also states:

“Measures should be taken to avoid personal data or files containing fixed data from being subjected to automatic transborder communication to third parties without the knowledge of the data subject.” (Clause 8.4)

7.6.12 At present our Privacy Act has no such protection. I make general recommendations in relation to transborder flows of personal data and will not repeat that material here. However, while noting that principle 3 contains a general prohibition on electronic transmission of personal information from public registers, there are three exceptions.¹⁸ I would be concerned if there were to be a great rush to place New Zealand public registers containing personal information on the Internet which would make personal information generally available in jurisdictions which have no privacy or data protection laws. Were that to happen, particularly if the ability to search was free of charge, I would have little doubt that databases on New Zealanders would be created in other jurisdictions. At the very least this would create the conditions for unwanted transborder direct marketing to New Zealanders. Certainly it would create the prospect of use of the information for purposes that were never intended when the information was obtained.

7.6.13 I recommend that further study be made of the issues and the means by which the law may be amended to better address the risks. One way in which the issue might be tackled would be for the reference to “member of the public” in the principle to be amended to refer to a “member of the public *in New Zealand*”. I expect that “member of the public” is probably normally understood to mean people in New Zealand in any case. One practical effect would be that personal information contained in public registers could not be made available for search on the Internet unless:

- there was a mechanism established for limiting searches to people in New Zealand; or
- principle 3 is modified by code of practice - in which I would consider relevant privacy issues such as the sensitivity of the data, the explanations that had been given to individuals at the time of collection, and the degree of compulsion used in obtaining the information;
- the electronic disclosure to overseas enquirers is authorised by an enactment.



RECOMMENDATION 88

Public register privacy principle 3 should be amended by adding “in New Zealand” after the words “a member of the public”.

¹⁷ Clause 6.1.

¹⁸ See sections 60(3) and 64(a) and paragraph 7.6.4.

7.6.14 In my view a restriction of this sort is justified to inhibit any rush to place public registers containing personal information on the Internet. It may be that satisfactory technical means can be developed to limit searches to all, or sensitive parts of, databases proposed to be placed on the Internet. If that is the case, electronic transmission will be permissible in conformity with the amended principle. In other cases, it will be open to the relevant department to seek statutory authority to place a public register on the Internet notwithstanding principle 3. Again, I see that as appropriate since Parliament is often a final arbiter between personal rights and public interests. Similarly, a department can promote the idea of a code of practice. Were a department to do so it ought to carry out a privacy impact assessment to show, amongst other things, how it is intended to:

- protect sensitive data;
- inform individuals whose information is to be made available as to the practice; and
- use technical means to limit the scope of electronic interrogations or searches with a view to preventing unauthorised downloading or consultation of personal information.

7.6.15 The recommendation that I have made is consistent with Recommendation R(91)10 to which Parliament has formally directed my attention. However, I anticipate that voices will be raised claiming that somehow the proposal unacceptably stifles innovation or new delivery of public services. Critics may argue that obtaining an amending Act of Parliament is too high a hurdle. Accordingly I propose that regulations be able to be issued under the Privacy Act to permit electronic transmission notwithstanding the proposed controls. Such regulations will take precedence over principle 3.¹⁹ The regulation making power should be exercisable only after consultation with the Privacy Commissioner.



RECOMMENDATION 89

If recommendation 88 is adopted, there should be a power in the Act to make regulations, after consultation with the Privacy Commissioner, in respect of any public register to authorise and control the electronic transmission of personal data which is not limited to members of the public within New Zealand.

7.7 PRINCIPLE 4 - Charging for access to public register

7.7.1 Public register privacy principle 4 states:

PRINCIPLE 4

Charging for access to public register

Personal information shall be made available from a public register for no charge or for no more than a reasonable charge.

7.7.2 Rights of access to personal information granted to individuals can be undermined if significant barriers are placed in the way through fees and charges. This is recognised in the procedural and complaints provisions attached to the information privacy principle 6 right of access²⁰ as well as by this principle.

Third party charging

7.7.3 However, this principle goes further than addressing just the matter of the individual concerned having access to personal information held on a register. It

¹⁹ See section 60.

²⁰ Generally speaking a public sector agency cannot make a charge for giving an individual access under information privacy principle 6. A private sector agency may only make a “reasonable charge”. Complaints concerning the reasonableness of a charge can be taken to the Privacy Commissioner for determination: see sections 35, 36 and 78.

also applies to third parties, such as direct marketers, seeking access to personal information held on a public register. In those circumstances a different set of issues arises. Keeping charges to third parties low or to a “reasonable” level does not necessarily protect or enhance privacy. Indeed, in some circumstances that could work against privacy interests if it means that commercial interests can, for no charge or for a very modest fee, obtain information which has been collected compulsorily which they could not obtain if they had to meet the costs of collection themselves.

- 7.7.4 I have concluded that principle 4 goes further than is necessary to protect privacy interests and by doing so it has the potential to place the Commissioner in the position of adjudicating on complaints about excessive charging for access to information the use of which is likely to be detrimental to an individual’s privacy. My qualms about exercising such a function arise because there is the potential for conflict with my privacy role. For this reason I consider that principle 4 should be amended to read as follows:

Personal information on a public register shall be made available *to the individual concerned* for no charge or for no more than a reasonable charge [change highlighted].



RECOMMENDATION 90

Public register privacy principle 4 should be amended so that the constraints upon charging for access to personal information from a public register apply only in relation to the making available of information to the individual concerned.

- 7.7.5 The agencies maintaining public registers could ensure compliance with the amended principle in a variety of ways. They could:
- make no charge for access to the register at all;
 - make no charge for access to the register by the individual concerned but levy a charge for a search by any other person;
 - levy a common charge for access by the individual concerned or any other person, set at a level that is “reasonable” in respect of the individual concerned;
 - make a lower charge for searches by the individual concerned than for others;
 - establish the charging regime by regulation - which would override the principle pursuant to section 60(3).
- 7.7.6 The proposal for partial “deregulation” would *not* require registrars to maintain a separate charging regime for requests by individuals if they did not wish to do so. It would be open to them to levy a higher charge for access by anyone other than the individual concerned.²¹ However, as now, registrars can simply keep all search fees to a reasonable level. In fact, I expect that charges in respect of a number of registers are set by regulations in any case. It would be open for individuals to complain to me under section 61(1) if regulations set charges which were excessively high.
- 7.7.7 I am suggesting that principle 4 not be the legal determinant of such matters. If public authorities wish to raise the costs to third parties of searches of public registers then this is, to my mind, a matter which can be satisfactorily determined outside the framework of the Privacy Act.
- 7.7.8 In respect of central government agencies, the approach to pricing presently recommended by Cabinet is contained in the State Services Commission *Policy*

“As it stands, this principle means that commercial entities are able to get information at far less than its market value and thereby make a profit, which is at the expense of the public in the end. Thus it is understandable that some local authorities should wish to recover this value for their citizens by charging something like a market rate. But if local authorities were enabled to charge a market rate they would have an incentive to use public registers in ways that are outside the purposes of the register; there would be a conflict of interest with their role as custodians of registers.”

- LOCAL GOVERNMENT NEW ZEALAND, SUBMISSION S51

²¹ This is the approach taken in some overseas legislation in respect of credit reference registers (although those would not usually be characterised as “public” registers). In some US states the individual is entitled under law to a free search each year or a search for no more than a set fee. Some laws, or proposed laws, also require that the charge made to the individual concerned not exceed the usual charge made to a customer of the credit reporting company.

Framework for Government-held Information which was finalised in 1997.²² Whether that approach appeals to public bodies outside the core state service, such as local authorities, would seem to be a matter for public policy formulation and the exercise of legislative and administrative powers. To the extent that this is a public register issue, it would seem undesirable to leave the matter solely to principle 4 and its reference to a “reasonable charge”.

7.8 PROPOSED NEW PRINCIPLE - bulk disclosures

7.8.1 It has been suggested that the existing principles do not get to grips with the full range of public register privacy issues and are therefore inadequate. The recommendations in respect of the four existing principles are intended to tackle their shortcomings and enhance their relevance and effectiveness. However, even with the recommended changes, there are significant privacy issues which for the most part remain unaddressed:

- there is patchy control of bulk searching of registers with resultant effects such as direct marketing and the creation of profiles on private databases;
- some registers are published in their entirety and sold, thereby ceasing to be under any effective control;
- although principle 3 does act so as to discourage bulk searching or copying of public registers, it does so indirectly and it does not openly confront and prohibit such practices.

The new principle I propose below seeks to address these problems.

Obtaining bulk information from a register

7.8.2 A constant refrain in submissions was the serious concern expressed at the release of bulk information from registers for commercial use - primarily direct marketing. The concerns expressed in submissions not only came from individuals or community groups, but also from the agencies maintaining public registers themselves. Particularly notable was the concern expressed by local authorities and organisations responsible for local government issues. A typical comment was made by Local Government New Zealand:

“Whatever for the most part the legal reasons may be whereby bulk information can be released for the commercial benefit of the recipients, such an outcome is clearly at odds with ... appropriate and laudable statutory purposes.”
(submission S51)

7.8.3 Certain registers have been revealed as having a commercial value and are subject to constant and continuing requests for bulk data which is used to create and sell lists which are used to direct market to the individuals concerned. One instance of this is found in respect of the use of the building consent register. Individuals who are erecting or altering a building must apply to their territorial authority for a building consent. Councils create weekly or monthly lists of the applications received and commercial interests regularly request these. As a result, the individuals who have applied for the consents receive, out of the blue, various solicitations to purchase building supplies, products or services. They have been given no choice. A number of territorial authorities have been reluctant to release such lists in deference to the privacy concerns of the individuals concerned but have been required to do so by the Ombudsmen. I have been consulted by the Ombudsmen on certain bulk requests and have opposed release on privacy grounds.

7.8.4 A similar issue arises in respect of the use of the valuation rolls or rates records whereby occupiers or absentee owners are approached by real estate agents. In June 1998 it was revealed that thousands of Auckland valuation records had

²² The full document is contained in a cabinet committee paper. The most easily accessible public version is to be found in the Law Commission, *Review of the Official Information Act 1982*, 1997 Appendix I.

been sold to a marketing company in Queensland, a jurisdiction having no privacy laws. In the first wave of marketing, Auckland property owners were the recipients of letters inviting them to “pay off your home loan four times faster without paying any more!!!” Press reports suggested “hard sell” tactics applied to those responding to the invitation. It was publicly reported that the bulk release of information, initially resisted by the department on privacy grounds, was prompted by the Ombudsmen’s office.²³ I had not been consulted on the matter by the Ombudsmen.

- 7.8.5 This issue has been canvassed in reviews of privacy law overseas. Several Canadian provinces have legislated to directly address the issue. For example, the Nova Scotia Freedom of Information and Protection of Privacy Act provides that a disclosure of personal information is presumed to be an unreasonable invasion of a third party’s personal privacy if:

“The personal information consists of the third party’s name together with the third party’s address or telephone number and is to be used for mailing lists or solicitations by telephone or other means.”²⁴

- 7.8.6 The Nova Scotia provision is repeated in other statutes. A new approach has been taken in a recent privacy law, the Freedom of Information and Protection of Privacy Act 1997 of Manitoba. That Act provides:

“Volume disclosure from a public register

The head of a public body shall not disclose to an applicant under this Part, personal information in a public registry on a volume or bulk basis.”²⁵

- 7.8.7 The Manitoba Act defines “public registry” as meaning a registry of information designated in regulations that is maintained by a public body and is available to the general public. It therefore closely resembles the concept of “public register” used in our own Act.

- 7.8.8 I consider that a principle modelled upon the Manitoba position would be a valuable addition to the public register privacy principles and directly address a problem which the other principles can only influence indirectly. However, I propose that it be modified by reference to the *purpose* for which a register is maintained - for example, to allow the accessing of the motor vehicle register to obtain hundreds of records relating to a faulty motor vehicle for a safety recall.

- 7.8.9 Accordingly, I suggest a principle which reads as follows:

PRINCIPLE 5

Bulk disclosures of information from public register

Personal information containing an individual’s name, together with the individual’s address or telephone number, is not to be made available from a public register on a volume or bulk basis unless this is consistent with the purpose for which the register is maintained.

- 7.8.10 The proposed principle is directed towards solicitation lists created directly from a register and therefore has features in common with the Nova Scotia provision. It is not an attempt to tackle the use of public registers to contribute public register profile details to mailing lists which already exist, because public

“The Committee believes that an individual’s privacy interest is not adequately protected where the person’s name, addresses, and telephone number can be made available for mailing lists. The Committee also objects to the use of public funds to finance access to information for private commercial purposes such as mailing list solicitation.”

- STANDING COMMITTEE ON THE ONTARIO LEGISLATIVE ASSEMBLY, REPORT ON THE MUNICIPAL FREEDOM OF INFORMATION AND THE PROTECTION OF PRIVACY ACT 1989, 1994

²³ “Ombudsmen order freed home details” *NZ Herald*, 26 June 1998.

²⁴ Freedom of Information and Protection of Privacy Act 1993 (Nova Scotia), section 20(3)(i).

²⁵ Freedom of Information and Protection of Privacy Act 1997(Manitoba), section 17(6).

register privacy principle 2 constrains that, to a certain extent, already. I have used the “volume or bulk basis” phrase from the Manitoba legislation. I believe that, for the most part, the agencies maintaining public registers generally have a good idea of the normal range of ordinary searches of the register. The marketing type requests are, I understand, relatively plain to identify, at least in respect of those registers currently facing such use. I have not framed the principle in terms of prohibiting the use of public registers for “direct marketing” although that may offer a satisfactory alternative.²⁶

7.8.11 The provision is similar to one very recently adopted in section 52(1)(f) of the Rating Valuations Act 1998 which allows regulations to be made:

“Prescribing limitations or prohibitions on the bulk provision of district valuation roll information for purposes outside the purposes of this Act or the Rating Powers Act or related legislation or to persons not having responsibilities in relation to the administration of this Act or the Rating Powers Act or related legislation.”

7.8.12 The principle also finds an echo in concerns recently expressed by the Electoral Select Committee over the purchase of electoral rolls and habitation indexes by businesses for marketing and debt collection purposes.²⁷

Publication of a register in its entirety

7.8.13 The discussion paper noted that there are circumstances in which a register may be dealt with, and disclosed, as a whole. For example, the agency maintaining the register might decide to publish the entire database as a book or in electronic form on CD-Rom. The publication may be made available for purchase so that anybody can possess the entire public register as at that point in time. An example is the electoral roll which is published at various points in the electoral cycle.

7.8.14 The discussion paper noted that some privacy risks arising from such publication include:

- the effect of disclosure may be multiplied over what would have been the effect of simply having the details placed on the register and available for a case by case search;
- the publication becomes available for use outside the control of the agency maintaining the register, for example, the entries can be electronically scanned into a database and used for profiling or marketing purposes;
- since many registers will be updated daily through additions and deletions, it is possible that printed versions in use may not be up to date;
- errors corrected on the official database will remain in printed copies earlier distributed;
- the complete version may be subject to re-sorting, or the addition of search references not intended or permitted for the original register.

7.8.15 The discussion paper canvassed the desirability of a principle prohibiting the publication or sale of a register in its entirety unless that publication or sale is necessary to achieve the purposes of the register. Considerable support for the proposal was offered in submissions. However, a number of submissions pointed out that the publication of a *significant portion* of a register would carry similar risks to publication of the *entire* register. I consider that the proposed principle will be satisfactory to address the concerns arising in relation to the publication or sale of entire or significant portions of registers as well as the bulk or volume searches for commercial purposes.

²⁶ The Act already has a definition of “direct marketing” in section 9 which could be utilised.

²⁷ Electoral Law Committee, *Interim Report on the Inquiry into the 1996 General Election*, April 1998, pages 32-33.

**RECOMMENDATION 91**

A further public register privacy principle should be enacted that provides that personal information containing an individual’s name, together with the individual’s address or telephone number, is not to be disclosed from a public register on a volume or bulk basis unless this is consistent with the purpose for which the register is maintained.

7.9 SECTION 60 - Application of information privacy principles and public register privacy principles to public registers

7.9.1 Section 60 requires every agency which is responsible for administering a public register to comply so far as reasonably practicable with the information privacy principles and the public register privacy principles. Where any such principle is inconsistent with any provision of any other enactment then, for the purposes of Part VII, that enactment will prevail.

7.9.2 The public register part of the Privacy Act is unusual in that it creates a regime that is not generally enforceable - although it may become so through the issue of a code of practice. Other sets of obligations created by the Act, such as in relation to the information privacy principles and information matching controls, can be taken on complaint to the Tribunal through the Act’s mechanisms.

7.9.3 It is also unusual that agencies which administer public registers are the only ones that need comply with the information privacy principles only “so far as is reasonably practicable”. Another unusual feature is that while public register privacy principle 2 applies to “any person”, this constraint upon use of personal information appears not to be enforceable like the general controls on use in information privacy principle 10.

7.9.4 In my view the position is unsatisfactory and anomalous. It is desirable for the application and enforceability of the public register controls to be brought more closely into line with the general approach of the Act. There were sound reasons in 1993 when the new public register regime was created to avoid a fully enforceable regime. However, that time is now past. To have the applicability of the principles, and remedies for aggrieved persons, put on a sounder basis will not in my view cause any significant difficulties. It would provide for a more satisfactory and effective regime for protecting privacy.

7.9.5 There are several approaches that could be taken to reforming this provision. For that reason, I will separately identify some of the problems or issues and suggest amendments which can be taken either as a package or as component parts. The key issues seem to concern:

- reconciling the application and savings provisions;
- reference to “every person” rather than “every agency”;
- use of “reasonable practicability” as the basis of an exception.

I address issues of enforceability at paragraph 7.10.

Application and savings provisions - sections 7, 8 and 60

7.9.6 The first issue to be addressed relates to the interaction between the savings provisions found in sections 7 and 60. Section 7(6) provides that:

“Subject to the provisions of Part VII of this Act, nothing in any of the information privacy principles shall apply in respect of a public register.”

7.9.7 Section 60, which is within Part VII, provides:

- in subsection (1), that the agency responsible for administering any public register must, in administering that register, comply “so far as is reasonably practicable” with the information privacy principles;

VII

s 60

251

“Our members were invited to comment to us on this review. Clearly the most important concern expressed was that public registers, particularly under the Building Act 1991 and the Rating Powers Act 1988, are being accessed by commercial organisations to obtain bulk information for direct marketing purposes. There is a widely held view amongst persons affected that this is a breach of their privacy.”

- LOCAL GOVERNMENT NEW ZEALAND, SUBMISSION S51

- in subsection (3), that where any information privacy principle is inconsistent with any provision of any enactment then “for the purposes of this Part of the Act” that enactment shall, to the extent of the inconsistency, prevail.

7.9.8 I know from various dealings over the years, and from consultation, that this interaction is a point of confusion for people who have considered public register privacy issues. It seems to me that amendment of sections 7 and 60 is desirable to make the combined effect plainer. In my view this can be achieved, in a straightforward manner, by several minor changes, the first of which involves substituting for section 7(6) a provision to read:

“The information privacy principles apply in respect of a public register to the extent specified in section 60 and section 63(2)(b).”²⁸

This of itself should not make any significant substantive difference to the way that the Act applies in this context. The new provision will primarily act as a flag in relation to the primary section. The subsection should probably be relocated into section 8 as it concerns the application of the principles rather than the saving of other laws.



RECOMMENDATION 92

Section 7(6) should be replaced with a subsection in section 8 providing that the information privacy principles apply in respect of a public register only to the extent specified in section 60 and 63(2)(b).

7.9.9 The second set of minor changes concern section 60 itself. The first point to note is that section 60(3) ties in directly with section 60(1), a point obscured somewhat by the interposition of subsection (2). A redraft should bring those two provisions together. Accordingly, the phrase “subject to sub-section (3) of this section” can be dropped (which is consistent with drafting changes adopted by the Parliamentary Counsel Office). It may be possible to re-draft section 60(3) more plainly. It would be desirable to drop the phrase “so far as is reasonably practicable” so as to more closely align the regime to that applying elsewhere in the Act.

7.9.10 Subsection (2) of section 60 provides that:

“Every person shall, so far as is reasonably practicable, comply with principle 2 of the public register privacy principles.”

“Every person” includes bodies which are exempted from the definition of “agency”. In my view, the words “every person” could be replaced with “every agency” in section 60(2) without creating any significant new privacy risks. I believe it is better that the relevant bodies be able to take the benefit of their usual exemption to the use controls of the Privacy Act.

7.9.11 Section 60, following these suggestions (and I make further suggestions below) could then be amended as follows:

- (1) Omit “subject to subsection (3) of this section” and “so far as is reasonably practicable”.
- (2) Subsection (1) does not apply where any information privacy principle or any public register privacy principle is inconsistent with any enactment and, in that event, the enactment prevails to the extent of the inconsistency.
- (3) The present subsection (2) - which could alternatively be subsection (1) - substitute “any agency” for “any person”.

²⁸ The reference to section 63(2)(b) encompasses the position established by a public register code of practice.

**RECOMMENDATION 93****Section 60 should be amended as follows:**

- (a) in subsection (1) omit the phrases “subject to subsection (3) of this section” and “so far as is reasonably practicable”;**
- (b) the content of subsection (3) should be moved adjacent to subsection (1) and redrafted in plainer fashion;**
- (c) in subsection (2) “person” should be replaced by “agency”.**

“Reasonably practicable” in section 60(2)

7.9.12 A further issue with subsection (2) is that difficulties could arise in relation to a use or disclosure complaint against an agency (other than an agency which administers a public register) if the action complained about involved a breach of public register privacy principle 2. For example, the agency may claim that there was an issue as to whether compliance was “reasonably practicable”. While relevant to the breach of the public register principle that phrase does not constitute an exception to either the use or disclosure principles.

7.9.13 In any case, it is not clear that “reasonable practicability” makes for a suitable exception relating to compliance. If exceptions are necessary it would be better, in my view, for these to be based upon specified public interests or individual authorisation as is the case with the exceptions to the information privacy principles. In my view the reference to “as far as is reasonably practicable” should be replaced by a reference to authorisation by the individual concerned and disclosure to that individual. Other public interests, if any, would be reflected in other legislation, the effect of which is saved by section 60(3).

**RECOMMENDATION 94****Section 60(2) should be amended:**

- (c) by omitting the words “as far as is reasonably practicable” and**
- (d) by substituting an exception based upon the authorisation of the individual concerned.**

7.10 SECTION 61 - Complaints relating to compliance with principles

7.10.1 Section 61 provides for complaint-initiated, or Commissioner-initiated, inquiries and investigations where it appears that:

- a public register provision is inconsistent with any of the information privacy principles or public register privacy principles;²⁹
- an agency administering any public register is not complying with the information privacy principles or public register privacy principles;³⁰
- any person is not complying with public register privacy principle 2.³¹

7.10.2 The Commissioner is given powers to carry out the inquiry or investigation which can result in a report to the chief administrative officer of the agency subject to the inquiry or investigation and may include recommendations for taking action to ensure greater adherence to the principles. It is clear from section 66 that such an inquiry or investigation cannot lead to proceedings before the Tribunal. However, if a code of practice is issued Tribunal proceedings can be taken in respect of certain actions which constitute a breach of that code.

7.10.3 There have been few complaints investigated under the public register privacy principles. There is little awareness yet of the existence of the principles or complaints mechanisms although expressions of dissatisfaction continue to ar-

²⁹ Sections 61(1), (2).

³⁰ Section 61(3)(a), (4).

³¹ Section 61(3)(b), (4).

rive at my office from individuals who are annoyed at receiving targeted marketing approaches using personal information obtained from registers. Although one inquiry is under way, most such matters have not led to formal investigations because:

- complainants lose interest when learning that complaints under section 61 can, at most, lead to a recommendation and not a remedy;
- complainants realise, after discussion with the Commissioner’s enquiries officers, that actions authorised or required by other legislation cannot be prevented by the operation of the principles.

7.10.4 In relation to section 60³² I canvassed the issue of whether the enforcement of the public register regime should be brought more closely into conformity with the approach taken to compliance with the information privacy principles by agencies generally. My recommendation is that the regime becomes fully enforceable in respect of agencies which administer public registers, and, in respect of principle 2, “any agency”. If my recommendation is not accepted then principle 2 should, as a minimum, be made enforceable in respect of any agency other than the agencies which administer the relevant public registers.

7.10.5 If all or some of these recommendations are accepted some resultant change will be necessary to section 61. In my view, it should be possible to amend section 61 to bring complaints or investigations under subsection (3) into the mainstream of the Act’s complaints mechanisms whereby matters could, if appropriate, be taken to the Complaints Review Tribunal. Most submissions supported this.³³ I consider that it would be inappropriate to do the same for subsections (1) and (2) since complaints of that type involve an inquiry into a provision in an enactment and may conclude with a recommendation as to the desirability of legislative action. These would be inappropriate functions for a judicial tribunal.

7.10.6 If the public register regime is to become enforceable it would generally be desirable, in my view, for this to be done by bringing the matters into the mainstream of the complaints mechanisms rather than creating further specific complaints procedures applicable solely in relation to public registers. Accordingly, in addition to any amendment to section 61 there will also be a need for consequent amendments to be made to certain other aspects of Part VIII which deals with complaints.



RECOMMENDATION 95

The public register privacy principles should be enforceable in a similar manner to the information privacy principles by amending, as necessary, sections 61(3) - (5) and 66.

7.11 SECTION 62 - Enforceability of principles

7.11.1 If complaints relating to public registers are brought into the “mainstream” with regard to enforceability and Tribunal proceedings, then it is possible that section 62 could be appropriately moved into section 11.

7.12 SECTION 63 - Codes of practice in relation to public registers

7.12.1 Section 63 provides for the Commissioner to issue codes of practice in relation to public registers. A code may modify the application of the public register privacy principles or the information privacy principles by prescribing stand-

³² See paragraph 7.9.2 and 7.9.4.

³³ Seven of the 9 submissions on the question agreed that complaints or investigations under section 61(3) ought to be able to be taken to the Tribunal (see submissions T1, T5, T6, T9, T12, T15 and S36). Submissions T17 and S42 did not support the proposition.

ards that are more stringent or less stringent than prescribed by those principles, or by exempting any action from any such principle, either unconditionally or subject to conditions that are prescribed in the code. A code may also prescribe how any one or more of the public register or information privacy principles are to be applied or are to be complied with or may “impose requirements that are not prescribed by any public register privacy principle”. A code may also provide for review and expiry. Procedures set out in sections 47 to 52 for Part VI codes are followed with any necessary modification.

- 7.12.2 Section 63(4) provides that to the extent that any public register code is inconsistent with any provision of any enactment, the code shall, to the extent of the inconsistency, be of no effect. This follows normal rules of statutory interpretation and would undoubtedly be the case even if subsection (4) had not been included. It is also consistent with the approach taken in sections 7 and 60 in relation to the status of the privacy principles as against other laws. However, subsection (4) is an important reminder as to the limits of what may be achieved by a code of practice particularly in the area of public registers where there is always another enactment - the one establishing the register - to take into account.
- 7.12.3 Given the significant privacy risks that I have outlined in relation to public registers it may be surprising that no public register codes of practice have been issued over the last four years. Reasons why no codes have been issued include:
- a code will be of no effect if inconsistent with other legislation - this has meant that it has been difficult to pursue effective codes which get to grips with the privacy issues where there appears to be a statutory obligation upon a registrar to give access to information without any discretion to withhold information for reasons of privacy;
 - even where the statutory interactions between the Privacy Act and the public register provision can be resolved there sits, in the background, the Official Information Act and the Local Government Official Information and Meetings Act which have the potential to undermine the approach taken by a code;
 - there has been the need to develop experience in the issues, and a coherent approach, which I believe my office now possesses;
 - other priorities have prevented significant resources being directed to the issues.
- 7.12.4 Although no code has been issued, preliminary work has proceeded on two prospective codes touching upon public register issues, including:
- a proposal for a code addressing the motor vehicle register - which was a spin-off from an earlier proposal for a broadly based law enforcement code which did not eventuate;
 - a proposed credit reporting code - which would require consideration of the issue of credit reporting companies utilising public register sources of information.
- 7.12.5 A credit reporting code proposal remains under consideration. Although considerable work was done on a proposed motor vehicle register code, progress was uneven. In 1997 work was discontinued on the code by my office and the LTSA and Ministry of Transport due to the opportunity to pursue privacy issues in relation to the motor vehicle register through primary legislation. This experience has been typical of a number of public register issues. It may be more straightforward, and ultimately more effective, to pursue matters through primary legislation where the opportunity exists than it is to seek to develop a code which may only be able to tinker at the edge of the privacy issues if the public register provision is at variance with a privacy solution.
- 7.12.6 Legislative reform of certain provisions establishing public registers or statutory

registers has been undertaken over the last four years. Some sound models for the reform of other register provisions have been enacted. The resultant provisions have either effectively addressed privacy issues or created an environment where, if necessary, a code of practice can usefully be issued.

- 7.12.7 A number of amendments to public register provisions made over the last five years have been mentioned elsewhere in this part of the report in relation to each of the public register privacy principles. However, I will mention here two examples where the resultant provisions acknowledge the possibility of a code of practice.
- 7.12.8 The first example is section 122ZI of the Local Government Act 1974. That provision created a new public register and set out the appropriate search references. However, in order to anticipate the possibility of the need to change search references at some future point the provision provided for the specifying of further search references by regulation. The section provided, as an alternative, that search references could be specified by code of practice. Therefore there will be no inconsistency with the statute if a code specifies further search references.
- 7.12.9 In respect of the Domestic Violence Act 1995 there is provision for aspects of the regime, such as the forms to be used, governing non-publication of information relating to protected persons to be spelt out by regulations or Privacy Act codes. In the broadly based Domestic Violence Act regime, which can apply to a large number of registers, it is possible that regulations might be issued specifically in respect of some registers, while others might be subject to a code of practice. The balance of the registers may find it entirely satisfactory to operate administratively without the need for aspects to be prescribed by either regulation or a code of practice.
- 7.12.10 It is anticipated that the most likely circumstance where the matters mentioned in the Local Government Act or Domestic Violence Act would warrant being effected by code of practice is where a code of practice is justified on privacy grounds anyway. The matters under consideration can then be incorporated into the relevant code of practice. The resultant code would be a combination of one issued under section 63 which is supplemented by the additional matters that can be done in those other provisions. I understand that I have powers to issue “combined” codes of practice of that type as was the intention when those provisions were passed.

7.13 SECTION 64 - Effect of code

- 7.13.1 Section 64 provides that where a code of practice in relation to a public register is in force, any action that would otherwise be a breach of a public register or information privacy principle is deemed not to be such a breach for the purposes of Part VII if done in compliance with a code of practice. Conversely, failure to comply with a code, even if it is not otherwise a breach of a public register privacy principle, is deemed to be a breach of a public register privacy principle.
- 7.13.2 This is similar to section 53 which states the effect of a code of practice issued under section 46. However, the importance of section 64 is that under current arrangements a code can put in place an enforceable regime whereby complaints can be taken to the Tribunal. In this respect the present regime differs from that in relation to codes issued under Part VI.³⁴

³⁴ The position is similar to that which applied in respect of Part VI codes during the transitional period following the introduction of the Act. See Privacy Act, section 79(3).

7.14 SECTION 65 - Power to amend Second Schedule by Order in Council

7.14.1 Section 65 provides for the addition of new public register provisions to the Second Schedule. The amendment is by way of Order in Council upon the advice of the Minister of Justice after consultation with the Privacy Commissioner.

7.14.2 In the five years to July 1998 the Order in Council route has not been used. Since the question of adding registers to the list has arisen during that period in the context of legislative proposals to create new registers, or amend the legislation governing existing registers, the Second Schedule has simply been amended by statute. However, in the light of the preceding discussion I am now of the view that a more systematic approach should be taken to bringing existing registers within the public register controls. The use of Orders in Council will provide a convenient mechanism to achieve this.

Use of Orders in Council to bring statutory registers into scheme

7.14.3 To bring all, or most, of the existing statutory provisions creating registers open to public search into the Second Schedule will require a process of:

- *identification* - locating the existing provisions in enactments;
- *evaluation* - considering, in conjunction with the agencies affected, any case for excluding a register from the regime;
- *making the order* - the process of preparing the order, consulting in relation to its wording, and finally issuing it;
- *implementation* - ensuring the new requirements are satisfactorily brought into effect.

7.14.4 I do not expect that the task of identifying the relevant provisions will be difficult. Many register provisions are amenable to straightforward computer searches of an electronic legislation database. Some obscure provisions may be overlooked at the early stages of any identification project but this, in itself, does not carry significant privacy risks.

7.14.5 The process of evaluation will be somewhat time consuming on the part of both my office and the Ministry of Justice. However, I am confident from experience since 1993, and examination of the issues in the course of this review by my office and the Ministry, that few significant problems should be encountered. The main challenge will be to engage the agencies which administer the registers in considering the issues, and to work through any implications for their registers. Many such agencies may have had no call previously to study the public register privacy principles and, human nature being what it is, will be cautious at the prospect of any set of statutory controls bearing upon them. However, I have found amongst officials who maintain statutory registers, a genuine interest in privacy issues and most are respectful of the privacy of people whose data they are entrusted with. Study of the matter by my office and the Ministry has not found any clear basis for the exclusion of any class of statutory registers from the scheme, but any agency would be free to make a case to keep its register outside the controls.

7.14.6 There is no need to have a single Order in Council to add all identified registers to the Second Schedule in one go. It would make most sense to undertake the task in batches. I suggest that the first Order in Council ought to be issued within 12 months of the start of the project of identification, with the whole task completed within two years. The nature of the grouping of registers in the Order in Council is not important from a legal or privacy perspective but would be a practical matter for the Ministry of Justice. However, there may be practical implementation issues which favour batching of Orders in Council by administering department or subject matter.

“It is submitted that statutory registers inherently can pose the same privacy concerns or risks as public registers. Such registers should therefore, be included in the Second Schedule to the Privacy Act 1993. This will ensure that there are privacy safeguards in place where any enactment, under which statutory registers are created, provides a discretion as to the purposes for which the information is to be used or released.”

- NURSING COUNCIL OF NEW ZEALAND, SUBMISSION T15

- 7.14.7 The last consideration is implementation of the public register controls within the agencies maintaining the new public registers. The process of consulting agencies in the preparation of the Order in Council will, I expect, quite effectively begin the compliance process. Ideally the Ministry of Justice will provide explanatory materials to the departments whose registers are proposed to be brought within the scheme. In the process of consultation those departments will begin considering the implications of the principles for their register and operation. The implications will be relatively modest and may not require immediate changes in practice in many cases. The Orders in Council should allow sufficient time before coming into effect to provide for any necessary operational changes.
- 7.14.8 The bringing of the additional statutory registers into the public register regime will provide an opportunity for timely general public education. For example, the ability for individuals who have a protection order under the Domestic Violence Act to obtain suppression directions on a significant range of registers is a matter that will need some co-ordinated information. The relevant advice needs to be available to professional advisers since individuals in such distressing situations are unlikely to know the full details themselves.

**RECOMMENDATION 96**

The Order in Council process in section 65 should be utilised to add existing register provisions in enactments to the list in the Second Schedule. The Ministry of Justice should commence work to identify the relevant enactments, and to consult with the relevant agencies, so that the first Order in Council is ready to be issued during the 1998/99 year with the completion of the project by the end of the following year.

Domestic Violence Act regulations

- 7.14.9 One of the issues that will need to be considered when further provisions are being added to the Second Schedule is whether the registers should also be brought within the scheme provided in Part VI of the Domestic Violence Act 1995 for the non-publication of information relating to protected persons on public registers.
- 7.14.10 This involves a consideration of separate issues to those involved in the decision to add a register provision to the Second Schedule. It should not be assumed that because a register is created as a “public register” it automatically follows that the domestic violence regime should apply. The critical reason to add a register to the domestic violence regime concerns whether an individual’s current whereabouts can be traced using the register. This primarily involves registers which display residential addresses. However, it may also be an issue for registers maintained on a district basis where appearance on a register indicates likely residence in that district (allowing further enquiries to pinpoint the location). In respect of existing public register provisions it has already been determined that it is unnecessary to add the drivers licence register to the domestic violence regime since it does not permit the location of individuals.
- 7.14.11 It would seem sensible for the question of the applicability of the Domestic Violence Act to be gone into in conjunction with the project to bring registered provisions within the Second Schedule.

**RECOMMENDATION 97**

The Ministry of Justice should, in carrying out the exercise to bring register provisions into the Second Schedule pursuant to section 65, also consider in respect of each register the desirability of issuing regulations under section 121 of the Domestic Violence Act 1995.

7.15 STATUTORY MECHANISMS FOR SUPPRESSION OF DETAILS ON REGISTERS

7.15.1 As will be apparent from this chapter, it is a difficult task to craft privacy provisions which can work in tandem with public registers. Generally a satisfactory approach will be one that reconciles the privacy interests with legitimate competing interests requiring disclosure of personal information. The approach I have generally advocated in this chapter has been to establish public registers with clearly stated purposes and to use controls, such as search references, to ensure that access is only given consistently with those purposes. However, sometimes there will be a need for an absolutely open and unrestricted search right and it is necessary to consider other safeguards in that context. One approach is to recognise that certain people have a particular need to have some of their details suppressed from general public search. A common example is the residential address of persons who have good reason to fear violence if they are located by a person who poses a real threat to them.

7.15.2 In any case, even where a regime has been fashioned to ensure that searches are only given for people having a legitimate “need to know” particular information, there may nonetheless be a case for a fall-back protection for people at risk. After all, it will be little comfort to a person who has been tracked down and attacked to know that the perpetrator may be prosecuted for having given a false declaration. Most of the chapter has been directed towards a regime that works reasonably well in a majority of cases to protect reasonable expectations of privacy. Where it comes to personal safety or harassment it is sometimes necessary to establish even stronger safeguards.

Suppression mechanisms in existing statutes

7.15.3 A suppression option has been adopted in several New Zealand statutes. The first example of which I am aware was the insertion in 1980 of section 62A into the Electoral Act 1956. This allows a person to enrol to vote but not to be named in the published electoral roll if that would be “prejudicial to the personal safety of the person or his family”. The provision has been carried over to section 115 of the Electoral Act 1993. A similar step was taken in section 19(5) of the Transport (Vehicle and Driver Registration and Licensing) Act 1986 to enable details to be withheld for reasons of “privacy or personal safety”. Suppression regimes exist in relation to registers open to public search maintained under the Radiocommunications Act 1989 and the Fisheries Act 1996. Sometimes other interests such as a fear of harassment, desire to preserve privacy, or national security, are specified.

7.15.4 Most significant of all such provisions are those contained in Part VI of the Domestic Violence Act 1995. A person who has obtained a protection order under that Act can apply for a direction from the agency which maintains a public register that identifying information on the register not be made publicly available. An elaborate set of provisions sets up the mechanism and allows for complaint to the Privacy Commissioner where an application for a direction is refused.

7.15.5 The provisions in the Domestic Violence Act can, in appropriate cases, be extended to any register maintained pursuant to a public register provision identified in the Second Schedule to the Privacy Act. Nonetheless there remain significant limits in protection of vulnerable people. The Domestic Violence Act, as its name suggests, only covers persons who have been the subject of, or fear, *domestic* violence. There are other people who have reason to fear violence if their whereabouts are easily able to be traced. These include, for instance, people, such as judges and police officers, whose occupation may bring them into contact with violent people. Witnesses and jury members may also sometimes be the subject of threats. Another group of people who might, in appro-

“Suppression of information which endangers a person’s safety does need to be addressed. The Domestic Violence Act provisions address part of the issue but we would value some provision to give us discretion to respond to an individual’s fear for their safety - an ability to block information on registers while other protections are put in place; a right to err on the side of caution.”

- FRANKLIN DISTRICT COUNCIL,
SUBMISSION T2

priate cases, benefit from being able to obtain a suppression direction are those who have been the subject of harassment.³⁵

Harassment

- 7.15.6 In my report on the Harassment and Criminal Associations Bill I suggested that consideration should be given to enabling people who obtain a restraining order under the Harassment Act to obtain a direction for suppression of details held on a public register in a manner similar to the scheme operated under the Domestic Violence Act.³⁶ In my report, I went through the issues in some detail and suggested that the objective might be achieved in one of three ways: (a) amend the Electoral Act and other specific provisions only; (b) extend the Domestic Violence Act scheme to victims of harassment; (c) tackle the issue more comprehensively.
- 7.15.7 There were pros and cons in relation to each of the options. Amending solely the Electoral Act would mean that the issue was only partially addressed. Extending the Domestic Violence Act scheme to victims of harassment would be confusing conceptually since it would treat a restraining order under the Harassment Act as a protection order for the purposes of Part VI of the Domestic Violence Act. Tackling the issue more comprehensively raised its own difficulties since it might involve discontinuing the Domestic Violence Act scheme which had only recently been created. The comprehensive approach also raised issues which were beyond the remit of the select committee studying the Harassment and Criminal Associations Bill.
- 7.15.8 The select committee studying the Harassment and Criminal Associations Bill adopted the first option and solely amended the Electoral Act. In doing so the Committee reported:

“The Privacy Commissioner expressed concern that victims who apply for restraining orders need their privacy protected, especially their home address and phone number. These details can be disclosed on public registers such as those under the Electoral and Births, Deaths, and Marriages Registration Acts.

“Section 115 of the Electoral Act 1993 allows the Chief Registrar to direct that a person’s name not be included on the electoral roll where publication would be prejudicial to his or her personal safety. Where a protection order under the DVA is enforced it is sufficient to produce the order, without having to produce any further evidence. The proposed restraining orders under the provisions in the Bill have a similar effect. Therefore, we recommend [a] new clause to amend the Electoral Act 1993 so that a restraining order made under the provisions in the Bill will be sufficient to justify the protected person’s name being placed on the unpublished roll.

“We note that the Privacy Commissioner suggested adapting Part VI of the DVA to enable people who obtain restraining orders to get directions that their personal details contained in public registers be held in a confidential list. We understand that as part of the Privacy Commissioner’s review of the Privacy Act 1993, a discussion paper will be

³⁵ Note that harassment does not always involve violence and is therefore not necessarily subsumed into any personal safety ground.

³⁶ See Report by the Privacy Commissioner to the Minister of Justice on the Harassment and Criminal Associations Bill (other than provisions dealing with interception warrants), 23 January 1997.

released in the near future relating to the public register provisions in the DVA. The discussion paper may make a recommendation that will affect Part VI of the DVA. Therefore, it seems preferable to *defer the decision* of incorporating a regime similar to that in the DVA until the outcome of the discussion paper is known. We consider it a preferable alternative to recommend the *interim measure* as outlined above.”³⁷ [Emphasis added]

- 7.15.9 I have taken the select committee’s report, particularly the portions highlighted, to indicate that they saw the amendment to the Electoral Act as an interim measure pending consideration of the merits and workability of some broader solution concerning suppression of details of persons who have obtained a restraining order. The committee rightly noted that as part of my review of the Privacy Act I would release a discussion paper relating to these issues.

Discussion paper

- 7.15.10 In the discussion paper the problem of people who feared violence, but who did not have a protection order, and those who had been a subject of harassment were outlined. Two questions were posed. The first asked:

“Should there be a public register privacy principle dealing with suppression of information in cases where it is established that an individual’s safety, or that of their family, will be put at risk through the availability of details of their whereabouts?”

- 7.15.11 Fourteen submissions were received. Ten answered yes³⁸ while only two answered no.³⁹ Two submissions did not directly answer the question but offered observations. One, from a district council, noted that the issue of personal safety needed to be addressed, that the Domestic Violence Act addressed only part of the issue, and the Council would value having a discretion to respond to an individual’s fear for their safety - “an ability to immediately block information on registers while other protections are put in place; a right to err on the side of caution.”⁴⁰ The other suggested a need to be cautious about extending Part VI of the Domestic Violence Act further before it had an opportunity to operate in practice for a while.⁴¹

- 7.15.12 A second question asked:

“As an alternative, or supplement, to creating a new principle dealing with personal safety, should Part VII of the Privacy Act contain mechanisms for obtaining suppression directions on public registers which would replace Part VI of the Domestic Violence Act but be applicable to a wider range of circumstances?”

- 7.15.13 As with the previous question, 14 submissions were received. Nine directly answered yes.⁴² No submissions answered no to the question. The other sub-

³⁷ Harassment and Criminal Associations Bill as reported from the Justice and Law Reform Committee, commentary, page vi. The Electoral Law Committee also supported the change. See Report of the Electoral Law Committee, *Interim Report on the Inquiry into the 1996 General Election*, April 1998, page 34.

³⁸ See submissions T1, T3 - T6, T9, T11, T12, S36 and S51. T4, T11 and S51 answered this question, and the following one, jointly in the affirmative.

³⁹ See submissions S42 and S58.

⁴⁰ Submission T2.

⁴¹ Submission T17.

⁴² See submissions T4, T5, T6, T9, T10, T11, S42, S51 and S58. T4, T11 and T51 answered the two questions jointly in the affirmative.

missions generally offered observations on the proposal but without opposing the course of action suggested. One expressed a preference for this proposal rather than the creation of a public register privacy principle as suggested in the previous question.⁴³ Another preferred mechanisms of the type contemplated in the question to be a supplement to a principle.⁴⁴ Others were unsure of the merits of one approach as against the other.⁴⁵

- 7.15.14 In my view, the issue should be taken forward. The two mechanisms canvassed in the discussion paper were the creation of a new public register privacy principle or the creation of a broadly based scheme for the obtaining of directions for suppression, modelled upon the Domestic Violence Act. A third possibility, anticipated in the second question, is to do both - create a new principle and use a suppression mechanism as a supplement. I have decided to recommend this third option.
- 7.15.15 I believe that a public register privacy principle and a statutory suppression scheme together will achieve more than simply doing one thing or the other. A principle, for example, will apply to all public registers listed in the Second Schedule whereas the suppression mechanism will be applied on a case by case basis only where appropriate. Sometimes the personal safety issues can be dealt with adequately without the need for the statutory suppression scheme. The statutory suppression scheme will prevail over inconsistent public register provisions whereas a principle will not.⁴⁶
- 7.15.16 In this report I do not set out all the detail of how this arrangement would operate. If a decision is taken by the Government to implement my recommendation there will be important work to be done on the detail and I will offer further views during that process. However, I outline the new principle that I propose and sketch out the broad details of how a broadly based statutory suppression scheme could be created.

Proposed new public register privacy principle

- 7.15.17 In devising a new principle directed to personal safety issues I have considered the Council of Europe Recommendation R(91)10 which I am directed to have regard to under section 13(1)(e) when reviewing the public register privacy principles. Clause 2.2 of those recommendations states:

“Unless domestic law provides appropriate safeguards and guarantees for the data subject, personal data or personal data files may not be communicated to third parties for purposes incompatible with those for which the data were collected.”

- 7.15.18 This provision does not explicitly refer to personal safety issues and, in a sense, simply restates the general approach to privacy issues. However, it does point out two things, the need for “safeguards” to be taken, and the point at which the risk is manifest, the communication of personal information to third parties for purposes incompatible with those for which the information was collected. Part 3 of Recommendation R(91)10 provides an approach for “sensitive data”. Strictly speaking this is not directed to data giving rise to risks of personal safety but instead to those categories referred to in article 6 of the Council of Europe Convention No 108.⁴⁷ However, it may suggest an approach when it states:

⁴³ See submission T9.

⁴⁴ See submission S42.

⁴⁵ See, for example, T1 and S36.

⁴⁶ See section 60.

⁴⁷ Article 6 refers to personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, and data relating to criminal convictions.

“Sensitive data

3.1 Personal data falling within any of the categories referred to Article 6 of Convention 108 should not be stored in a file or in part of a file generally accessible to third parties.

Any exception to this principle should be strictly provided by law and accompanied by the appropriate safeguards and guarantees for the data subject.”⁴⁸

7.15.19 Accordingly, I have devised a new public register privacy principle which directs agencies maintaining public registers to keep certain details stored separately from information generally accessible to third parties with an exception where appropriate safeguards are in place. Agencies should have a process whereby individuals with special safety concerns can ask to have the details of their whereabouts held in a non-accessible part of the database. Those details would only be released with a great deal of care to ensure that the information was not to be used for an incompatible purpose. An agency would not need to segregate such details if appropriate alternative safeguards addressed the risks involved. The proposal would not require *all* information to be held separately, only that revealing an individual’s whereabouts.

7.15.20 The proposed new principle might appear along the following lines:

*PRINCIPLE 6**Personal safety or harassment*

- (1) Where practicable, personal information revealing an individual’s whereabouts should not be stored in a part of a register generally accessible to the public where it is shown, on an application by the individual to the agency maintaining the register, that the individual’s safety or that of the individual’s family, would be put at risk through the disclosure of the information.
- (2) An agency maintaining a public register shall have reasonable procedures to invite, evaluate and determine applications by individuals whose personal safety may be put at risk by disclosure.
- (3) It is an exception to clause (1) of this principle where other appropriate safeguards are taken to ensure that the information is not disclosed to the public for purposes unrelated to the purposes for which the information was collected or obtained.

7.15.21 I consulted on the *proposition* that there be such a principle but not on the draft principle itself set out above. The detail of the approach to be taken, and the drafting of the provision, would need to be the subject of consultation with agencies maintaining public registers. Accordingly, I have framed my recommendation in terms of the adoption of a suitable principle rather than the adoption of the actual principle suggested above. There may be other satisfactory ways of drafting a principle to achieve a similar purpose.

“Most state legislation in Australia contains express provisions that residential address is not to be part of the register of nurses available for inspection by the public.”

- NURSING COUNCIL OF NEW ZEALAND, SUBMISSION T15

⁴⁸ Clause 3.2 is not relevant for present purposes relating to the making available of sensitive categories of data, as outlined in Convention No 108, concerning public figures.

**RECOMMENDATION 98**

A new public register privacy principle should be created which obliges agencies maintaining public registers to adopt a process to hold details of an individual's whereabouts separately from information generally accessible to the public where it is shown that the individual's safety or that of the individual's family would be put at risk through the disclosure of the information. An exception is to be provided where alternative safeguards exist to ensure that such information is not disclosed to the public for purposes unrelated to the purposes for which the information was collected or obtained.

Mechanism for obtaining suppression directions

- 7.15.22 Over the last few years my office has made a number of suggestions for improving individual public register provisions as they come up for enactment or re-enactment. Often the best solutions, which provide for a free flow of information for legitimate uses but otherwise gives adequate privacy protection, are crafted in relation to particular registers in their own special circumstances. However, a register-by-register approach is inadequate to fully address either privacy or personal safety concerns. Unless some minimum privacy and personal safety protections are established across the board in relation to registers, the very good regimes established in one context may be undermined by the lack of safeguards in others. For example, an abusive partner may go to extraordinary lengths to seek to trace an estranged partner. It will not be sufficient to provide protection in relation to the electoral roll and motor vehicle register if, knowing the partner's assets, affiliations and personal interests, the violent person can nonetheless trace the individual easily through other registers.
- 7.15.23 In suggesting the regime now established in the Domestic Violence Act I was inspired by a scheme that had been conceived, but not implemented, in New South Wales. The Privacy and Data Protection Bill 1994 in that State proposed a very simple clause to establish a generic suppression regime. It stated:

“Suppression of information

- 20(1) A person about whom personal information is contained, or proposed to be placed, on a public register may apply to the record-keeper to have the information removed from, or not placed on, the register as publicly available and not disclosed to the public.
- (2) However, information that is removed from, or not placed on, the register as publicly available is to remain on the register for other purposes.
- (3) Despite the provisions of any other Act, the record-keeper may agree to the application if the record-keeper is satisfied that suppression of the information would not unduly compromise the register and the record-keeper is also satisfied that the applicant's safety or the safety of members of the applicant's family may be at risk if the application is not granted.
- (4) An applicant who is aggrieved by a decision of a record-keeper under this section may complain to the Privacy Commissioner under section 23.
- (5) In dealing with the complaint, the Privacy Commissioner may recommend that the record-keeper agree to the application or may notify the complainant that, in the Commissioner's view, the application was properly refused.
- (6) A record-keeper must comply with a recommendation by the Privacy Commissioner under this section.”

- 7.15.24 That simple provision provides an interesting contrast with the 17 section Part



VI of the Domestic Violence Act.⁴⁹ The New South Wales provision has not been implemented and therefore it cannot be known whether it would have worked satisfactorily without the degree of detail set out in the New Zealand Act and Regulations. Nonetheless, the degree of detail in the Domestic Violence Act serves as a warning as to the need to avoid unduly further complicating matters. Furthermore, I am keen to maintain the Privacy Act as “user friendly” as possible and would wish to achieve the objective with the least complexity possible.

7.15.25 Being mindful of issues of complexity, the desirability of avoiding duplication and the need for effective protection, I have concluded that the following features would probably make for the most effective and straightforward regime:

- a single generic suppression regime which is located in an appropriate statute - this leads me to recommend that the existing Domestic Violence Act regime be subsumed in a generic scheme to be in the Privacy Act;⁵⁰
- the Domestic Violence Act regime should remain as far as possible unchanged albeit relocated into another statute;⁵¹
- the detail of the scheme, presently found in Part VI of the Domestic Violence Act, to be placed in a schedule to the Privacy Act rather than in Part VII of the Act itself;⁵²
- opportunities should be taken to simplify some of the provisions from the Domestic Violence Act scheme - primarily in relation to links to the Privacy Act’s Second Schedule and complaints processes;
- directions for suppression should cover circumstances presently contemplated by the Domestic Violence Act (evidenced by individuals having obtained protection orders) and extend to other personal safety and harassment cases - with harassment cases being substantiated by the production of a restraining order and others substantiated in some suitable manner such as is provided for in section 113 of the Electoral Act 1993.

7.15.26 A number of practical and consequential issues would need to be worked through in transferring the regime from the Domestic Violence Act and satisfactorily providing for other cases of personal safety and harassment. For example, existing regulations may need to be carried over in some way. It would also make sense for the Second Schedule of the Privacy Act to be reformatted so that it is clear at a glance which public register provisions have also been brought within the suppression regime.



RECOMMENDATION 99

A mechanism should be established in Part VII of the Act, with the details set out in a new schedule, enabling individuals to obtain suppression directions in relation to public registers which would replace Part VI of the Domestic Violence Act but be applicable to a wider range of circumstances concerning personal safety and harassment.

7.16 INTERACTION WITH OFFICIAL INFORMATION ACT AND LOCAL GOVERNMENT OFFICIAL INFORMATION AND MEETINGS ACT

7.16.1 I cannot conclude the discussion of public registers without noting that the

⁴⁹ Part VI of the Domestic Violence Act also has to be read in relation to relevant regulations. The Domestic Violence (Public Registers) Regulations 1996 runs to 14 clauses and a schedule.

⁵⁰ I see the Domestic Violence Act and Harassment Act as inappropriate places to locate a generic regime as did officials advising the select committee on the Harassment and Criminal Associations Bill. A suitable alternative, but beyond my terms of reference, would be to create a stand-alone statute. One shortcoming of a stand-alone statute would be continuation of some complexity in cross referencing to the Privacy Act’s Second Schedule and my complaints jurisdiction.

⁵¹ This should offer least disruption to agencies maintaining public registers.

⁵² This should offer least disruption to regular users of the Privacy Act.

“Our members strongly share the concern about individual privacy. However, as managers of various public registers they have little option under the present law and administrative arrangements but to disclose bulk information for extraneous purposes. This places our members in a most invidious position.”

- LOCAL GOVERNMENT NEW ZEALAND, SUBMISSION S51

interaction with the official information statutes in this context has been problematic. Thus far in the chapter I have not directly addressed a recommendation to that inter-relationship.

- 7.16.2 Essentially a public register is an enactment which provides for access to personal information on a particular register. The information is usually also “official information”. Invariably public register provisions set out an entitlement to have access to information. Generally such provisions also describe the information to be made available. Sometimes a provision prescribes information that is not to be made available or place constraints upon subsequent use. Frequently, but not invariably, public register provisions outline the manner in which information is to be made available.
- 7.16.3 I believe that the inter-relationship between the Privacy Act and public register provisions, with the changes that I propose, is fairly satisfactory. The position is that a public register provision which expressly authorises or requires some action will prevail over the public register privacy principles and the information privacy principles. It will continue to do so under my proposals.
- 7.16.4 However, the position is made unsatisfactory by the fact that the official information statutes are not sufficiently clearly ousted from application to public registers. The intrusion of those statutes into matters which are specifically addressed by legislation in public register provisions and in the public register privacy principles is problematic, confusing and, in my view, quite unnecessary. The use of official information statutes by commercial interests to force the release of bulk information from registers makes the resolution of privacy concerns very difficult. I do not see the public interest as being served by bulk disclosures being forced on registrars and individuals in the name of “freedom of information”. There is, in my view, no public interest to be served by the disgorging of compulsorily obtained personal information to enable the preparation of marketing lists. Continuing “rulings” that such information must be handed over may bring the Official Information Act into disrepute.⁵³
- 7.16.5 I hesitate to prescribe precise solutions to the problem because they will affect not only the Privacy Act but also the official information statutes themselves. I am a firm supporter of open government and the aims of the Official Information Act but it seems to me that in this context something needs to be done to avoid the Official Information Act being used to upset any carefully crafted balance established in the public register provisions in particular statutes and under the public register privacy principles. The answer I suspect may be found in the interpretation of the savings provisions in the Official Information Act and the Local Government Official Information and Meetings Act or in their amendment.⁵⁴ A more limited proposal would make the official information statutes subject, in respect of public register provisions, to the proposed bulk release principle, thereby leaving untouched the position in respect of searches for individual records.



RECOMMENDATION 100

The official information statutes should be excluded from questions of release of personal information from public registers.

⁵³ In some cases the ruling may merely be the opinion of the Ombudsman that the official information legislation does not apply but that in his opinion the Act governing the register can be interpreted as requiring the bulk disclosure of the data.

⁵⁴ See, in particular, Official Information Act 1982, section 52(3)(b)(ii) and Local Government Official Information and Meetings Act 1987, section 44(2)(b)(ii).

Part VIII

VIII

Complaints

267

“The lack of resources is a serious issue because over time it could undermine credibility of the Office and, ultimately, the aims of the legislation.”
- NZ Law Society Privacy Working Group, submission UV18

“Complaint outcomes can provide useful examples to educate the public and agencies on the law. Complaints serve to keep the Commissioner aware of the difficulties agencies and individuals are having in relation to personal information. In addition, complaints provide an overview which may highlight difficulties within particular industries which need to be addressed.”
- Health and Disability Commissioner, UV16

“It makes sense, particularly with employment-related complaints, to continue the present low-level disputes resolution process which a privacy investigation essentially represents. Taking a complaint to the District Court would involve a great deal more time and expense for all parties and would by-pass the mediation process which has achieved some success.”
- NZ Employers Federation, submission UV4

“A complaints procedure is clearly the most accessible and barrier free approach to seeking redress.”
- Ministry of Justice, submission UV15

“The Commissioner’s Office would become far less effective in its educational role if it was denied the experience that dealing with complaints on a day to day basis provides. By being involved at the coal face, the Commissioner’s Office is able to detect new trends early on and take action to educate the public about such issues.”
- Telecom New Zealand, submission UV13

8.1 INTRODUCTION

8.1.1 Provision for enforcement of rights and entitlements is an essential feature of any credible privacy or data protection law. It is not enough simply to have a set of privacy principles and to apply these to agencies. It is necessary to have a system to ensure that there is some reasonable compliance with those principles and to call an agency to account for its actions which may constitute a breach of those principles. Jurisdictions approach the question of enforcement in a variety of ways. Some countries allow individuals to sue through the regular courts.¹ Euro-

¹ Most jurisdictions do not favour this option. However, the USA allows individuals to take proceedings through the courts under the Privacy Act 1974 in relation to public sector agencies.

pean countries pursue enforcement through a registration or licensing system with a mixture of criminal and civil sanctions for failure to register or for a breach of the law or conditions on a licence or registration. Many also provide for complaints through independent data protection or privacy commissioners.

New Zealand complaints model

- 8.1.2 The approach set out in the Act, and particularly in this Part, is to provide for complaints to be made to an independent and specialist entity, the Privacy Commissioner. An emphasis is placed upon low-cost, non-adversarial and timely resolution of complaints. The process is modelled upon that of the Ombudsmen which was pioneered in New Zealand under the Ombudsman Act 1962.
- 8.1.3 However, an Ombudsman-type complaints process does not itself lead to a binding legal determination of a complaint.² If the Privacy Commissioner's recommendations are not accepted a complaint may progress to the Complaints Review Tribunal which has powers to issue binding determinations, compensation and enforceable orders. There is also limited provision for certain access complaints to be taken to the courts.³ Although there are some aspects of the complaints processes which are new or unique to the Act, by and large they follow an existing model which has been used in New Zealand by the Ombudsmen and the Human Rights Commission and since copied into the Health and Disability Commissioner Act 1994.
- 8.1.4 The complaints processes under the official information legislation are the most direct forerunner of Part VIII. The part of the Official Information Act concerning access by individuals to personal information was transferred into the Act and the processes for access complaints were, by and large, also seen as suitable for the complaints involving breaches of other information privacy principles. However, there is no Tribunal in the Official Information Act arrangements and this aspect of the scheme is derived from arrangements under the Human Rights Act.⁴
- 8.1.5 The influential report of the Committee on Official Information ("Danks Committee") made various recommendations as to the mechanisms for enforcement under the Official Information Act which have in effect also shaped aspects of the Privacy Act years later. For that reason I have referred back to the Danks Report in this review and will mention aspects of it in the section by section discussion. The Danks Committee took the view that there must be in the information law a channel for public grievance. It took the view that "decisions about disclosure of information taken by departments and agencies must be subject to test by an independent arbiter."⁵ In a variety of ways the Committee's ideas continue to be reflected. In this review, I have gone back to the Danks report, not only to remind myself of the Committee's insights, but also to reconsider whether the ideas crafted for a law dealing only with access, and only in the public sector, should be rethought in the broader based Privacy Act.

Role of the courts

- 8.1.6 Danks advised against creating legal rights to information and that approach has generally continued with the recourse to the Commissioner and the Tribunal rather than regular courts. The Committee did propose giving individuals a *right* of access to certain specific categories of information in the public sector and that too is continued in the Act at section 11.

² Although in the official information context the Ombudsmen are the final arbiters on such complaints subject to Ministerial veto.

³ Privacy Act, section 11.

⁴ At the time that the Privacy Act was enacted the Human Rights Commission Act 1977 was in force. Under that legislation there had been recourse to a Tribunal, earlier called the Equal Opportunities Tribunal, for many years.

⁵ Committee on Official Information, *Towards Open Government: General Report*, paragraph 98.

- 8.1.7 It is interesting to reflect on one indicator of the success of the framework for complaints established under the Act. That is, that a litigation alternative exists for a significant class of complaints and yet that alternative is almost invariably not chosen by complainants. For complaints concerning a denial of access to information held by a public sector agency, which remain a large part of my complaints load, the matters may be taken directly to the regular courts.⁶ This continues the position under the Official Information Act. However, under both statutes citizens have preferred the processes provided by the Ombudsmen, and now Privacy Commissioner and Complaints Review Tribunal. Litigation is generally an unattractive and inefficient means to review a decision to withhold information.
- 8.1.8 However, the courts do have one role which will not be referred to again in this part of the report. People charged with criminal offences have a particular interest in having access to information held by a law enforcement agency. At present, we have no criminal discovery or criminal disclosure legislation and the obligations on law enforcement agencies to give access to information, and the role of the courts in supervising that, is largely underpinned on a statutory basis by the right of access granted in the Privacy Act. Courts determine these matters with implicit reliance upon the provisions of the Privacy Act taken together with those in the Official Information Act (for official information which is not personal information about the requester) and in reliance upon certain common law duties upon prosecutors to ensure a fair trial.
- 8.1.9 Where a prosecution has commenced, and the police have withheld information from a requester, requests for review are normally handled by the criminal court seized of the matter rather than by complaint to me and on to the Tribunal. If an individual was not legally represented and, instead of taking the matter up with the court, directed a complaint against the prosecuting agency to me, I would probably decide to take no action on the complaint under section 71(1)(g) (there being an adequate remedy that it would be reasonable for the individual to exercise). The court has various powers to ensure that disclosure is made and to delay a substantive hearing until that happens. There is currently a proposal for a statutory criminal disclosure regime which I believe would better provide for the handling of access matters during and in relation to criminal proceedings.⁷
- Complaints or reviews?*
- 8.1.10 The subject of Part VIII is, as its heading suggests, “complaints”. In fact, at various places the Part makes a distinction between complaints and Commissioner-initiated investigations. There is little or no substantive or procedural difference. However, one legal correspondent has raised the matter and there may be a case for the heading to Part VIII to read “Complaints and investigations”.
- 8.1.11 The Part makes no procedural distinction between complaints alleging a breach of information privacy principle 6 and complaints alleging a breach of any of the other principles.⁸ However, there may be a small advantage in relabelling complaints involving a decision to refuse a request under information privacy principle 6, as access “reviews”.
- 8.1.12 The point is a semantic one and is not related to a problem or difficulty in applying the Act satisfactorily. The issue simply is that “complaint” has certain negative connotations which in many cases are not justified in respect of complaints concerning a denial of access. The fact is, when an individual is denied

⁶ Privacy Act, section 11(1).

⁷ See submission by the Privacy Commissioner to the Ministry of Justice and the Department for Courts in relation to a consultation paper regarding Preliminary Hearings and Criminal Disclosure, February 1998.

⁸ A distinction is made in section 66(2) between these classes of complaints as there is no equivalent to section 66(1)(b) in subsection (2).

“The Commissioner plays an important role in resolving complaints. While forcing complainants to go direct to the Tribunal would result in a body of case law about privacy law being built up fairly quickly, it would discourage many complainants from seeking redress and be more costly for all parties concerned.”

- TELECOM NEW ZEALAND,
SUBMISSION UV13

access to information, he or she is not in a position to know whether that information has been properly withheld or not. By taking the matter up with my office the complainant can have the issue reviewed by an independent person to see if my opinion accords with that of the agency.

- 8.1.13 That is in contrast to complaints involving the other information privacy principles, public register privacy principles and information matching controls, where the individual really is alleging that the agency has done something wrong. The contrast is further marked in cases where the agency has withheld information to protect the privacy of another person.
- 8.1.14 It is possible that by calling the principle 6 complaints “access reviews” a slightly less confrontational mood might be engendered in the investigation. I have no evidence that this would indeed be the case but it seems a reasonable supposition. The agency would not be informed that a complaint had been made against it but merely that the individual had requested a review of its decision to withhold information. Some overseas information laws refers to “complaints” and “reviews”.⁹ Reference to “complaint” continues the terminology adopted by Danks and used in the Official Information Act.
- 8.1.15 Notwithstanding the possible merits of any changes in terminology I make no recommendation for amendment at this stage.
- 8.1.16 Appendix J sets out a series of graphs which illustrate some aspects of the receipt and disposal of complaints since 1993.

SECTION BY SECTION DISCUSSION

8.2 SECTION 66 - Interference with privacy

- 8.2.1 Section 66(1) defines the circumstances in which an action is an “interference with the privacy of an individual”. In essence (and with an important qualification in respect of access and correction matters) to qualify as an interference with privacy there must be:
- an action which breaches an information privacy principle; or
 - an action which breaches a public register code of practice;¹⁰ or
 - non-compliance with Part X (which relates to information matching);
 - taken together with some actual or possible adverse consequence of the action in question.
- 8.2.2 Subsection (2) provides that an action is an interference with the privacy of an individual if it involves certain decisions relating to an information privacy request and there is no proper basis for that decision. In other words, with respect to access and correction matters, subsection (2) does not contain the reference to the actual or possible adverse consequences that subsection (1) does.
- Clarification of interaction between subsections (1) and (2)*
- 8.2.3 Some confusion has arisen over the question of whether, on a complaint concerning refusal of access to personal information, there has to be shown to have been some kind of adverse effect upon the requester to constitute an “interference with privacy”. I am confident that section 66(2) was intended to ensure that substantiated access complaints could be considered an “interference with privacy” without any harm or detriment of the type referred to in section 66(1)(b)

⁹ See Freedom of Information and Protection of Privacy Act 1992 (British Columbia), section 42(2) and 52.

¹⁰ See recommendation 95 which proposes that breaches of the public register privacy principles should also found an interference with privacy.

so long as the various criteria in section 66(2)(a) and (b) are present. However, if there was some harm or detriment, a breach of principle 6 could alternatively be brought under section 66(1).

8.2.4 It is extremely important to ensure that there are enforceable remedies for the access entitlements in principle 6 without any proof of harm or detriment. Quite frequently, such harm or detriment will be absent. The absence of proof of harm must not exist as a barrier to enforceable rights of access. Were that to happen, it would significantly undermine the entitlement and be quite out of keeping with what was intended by the Privacy Act and what is expected by the OECD Guidelines and other international norms governing access laws. It would reduce rights formerly existing in the Official Information Act, and this was surely never intended.

8.2.5 Nonetheless, it is understandable that the confusion has arisen. The interpretational problem is derived from the fact that section 66(1) commences by stating:

“For the purpose of this part of the Act, an action is an interference with the privacy of an individual if, *and only if*, ...”.

On the other hand, section 66(2) commences:

“*Without limiting subsection (1) of this section*, an action is an interference with the privacy of an individual ...”.

8.2.6 In two early cases the Tribunal took the view that it needed to consider whether there had been some loss, detriment, etc under section 6(1)(b) for there to be an interference with the privacy in a case where information had been withheld. In my view, the Tribunal was wrong and it has, in fact, resiled from the position in all its recent cases.¹¹ The Tribunal has now explicitly held that pursuant to section 66(2) there is no need for evidence as to any damage to be established.¹²

8.2.7 I believe that it would be desirable to clarify the section notwithstanding that the confusion caused by the Tribunal’s earlier decisions has now been put right by the Tribunal itself. This may be achieved by deleting the phrase “and only if” from section 66(1). However, Parliamentary Counsel’s opinion should also be sought as to whether any other or further change is necessary to make the position more plain in any other way.



RECOMMENDATION 101

Section 66(1) should be amended by deleting the words “and only if”.

8.3 SECTION 67 - Complaints

8.3.1 Section 67 provides that any person may make a complaint to the Privacy Commissioner about an alleged interference with privacy.

8.3.2 A complaint may also be lodged with an Ombudsman who must forward the complaint to the Commissioner. The reason for this provision was that up until the enactment of the Privacy Act the Ombudsmen had been receiving and dealing with complaints concerning refusal of access to personal information held in the public sector and it was considered likely to cause less confusion for the Ombudsmen to continue to receive them for transfer to the Commissioner.

¹¹ For example, *M v Ministry of Health* (1997) 4 HRNZ 79, *M v Police* (1997) 4 HRNZ 91, and *Adams v NZ Police* CRT decision No. 16/97.

¹² For example in *M v Ministry of Health*.

- 8.3.3 It is timely to now repeal subsections (2) and (3) as there is no continuing need to expressly provide for the lodging of complaints with the Ombudsmen. The proportion of such complaints being received and passed on in this way has diminished as the public became more familiar with the Privacy Act and the respective roles of the Ombudsmen and Privacy Commissioner. Very few, if any, complainants complain to the Ombudsmen in reliance upon section 67. Rather, they complain to the Ombudsmen mistakenly thinking that they are the review authority for such complaints. There is no need for a provision such as subsections (2) and (3) since the complainants who enquire before lodging a complaint are easily directed to the correct complaints authority; and complaints wrongly received by the Ombudsmen may simply be transferred to my office pursuant to section 17A of the Ombudsmen Act.



RECOMMENDATION 102

Section 67(2) and (3) which provide for the lodging of complaints under the Privacy Act with the Ombudsmen, and for the transfer of such complaints, should be repealed.

8.4 SECTION 68 - Mode of complaint

- 8.4.1 Complaints may be made to the Commissioner orally or in writing. If an oral complaint is made, it must be put in writing as soon as practicable and if necessary my office is to render reasonable assistance.
- 8.4.2 My office is geared to render assistance but, in fact, oral complaints are rare. Usually in such cases the details are taken on the telephone, written down and subsequently checked with the complainant. Since the first year of operation of the Act I have maintained a freephone privacy hotline. This service helps ensure that complainants who are unable to make their complaint in writing nonetheless have equitable access to the complaints process wherever they live.

8.5 SECTION 69 - Investigation of interference with privacy of individual

- 8.5.1 My functions under this Part of the Act are:
- to investigate an action that appears to be an interference with the privacy of an individual;
 - to act as conciliator in respect of any such actions;
 - to take such further steps as are contemplated under Part VIII.
- 8.5.2 I may commence an investigation either on a complaint or on my own initiative. The overwhelming majority of investigations are commenced with a complaint. However, on occasion, I will initiate an investigation based on other information. For example, I may become concerned at an agency's actions through information received from the public or reported in the news media. It is also possible that I may initiate an investigation on my own initiative where a number of people complain about the same issue but not the individual concerned.
- 8.5.3 On one occasion there had been widespread news media reporting of an unauthorised disclosure of information. I expected a complaint to eventuate but, after a period, none arrived. Given the seriousness of the circumstances I initiated an investigation and, having established certain details from the agency, spoke with the individual concerned. It transpired that the individual was illiterate and had not been fully aware of aspects of the public disclosure or in a position to complain.

“A third party should be able to make a complaint. Some people lack the ability to make a complaint or would be too overwhelmed to make a complaint.”

- NZ LAW SOCIETY

PRIVACY WORKING GROUP,

SUBMISSION UV18

8.6 SECTION 70 - Action on receipt of complaint

8.6.1 Section 70 provides that on receiving a complaint, the Commissioner may decide either to investigate or to take no action on the complaint. I must advise the complainant and the agency complained about as soon as practicable of the procedure that is proposed to be adopted.

Notification

8.6.2 Section 70(2) provides for the Commissioner to advise the complainant and the “person to whom the complaint relates” of the procedure to be adopted. I take this latter phrase to mean the respondent, or the person who would be the respondent if proceedings are taken, as this is consistent with the way that the phrase is used in section 73(a).

8.6.3 An interesting point about the section is that it appears to require notification to the “person to whom the complaint relates” of a decision to take no action on the complaint. It might seem surprising to notify the agency that the Commissioner has received a complaint that he does not intend to investigate. Where a decision is taken not to investigate a complaint under the Human Rights Act notification is required to be given only to the complainant.¹³ Similarly, under the Ombudsmen Act only the complainant, and no-one else, is required to be notified.¹⁴

8.6.4 I suspect that it may have been unintentional to require notification to the agency where a decision is taken to take no action on a complaint. It is, for example, somewhat mysterious to advise an agency out of the blue of “the procedure that the Commissioner proposes to adopt” in relation to a complaint in respect of which the Commissioner intends to take no action. Furthermore, section 71, which precisely sets out the grounds upon which the Commissioner may decide to take no action, expressly states that the Commissioner is to notify the complainant of the decision to take no action, or no further action, and the reasons for that decision. It is silent in relation to the respondent agency.¹⁵

**RECOMMENDATION 103**

Section 70(2) should be amended so that the Commissioner is obliged to advise of the procedure to be followed only where he has decided to investigate a complaint so as to avoid overlap with the obligations in section 71(3).

Deferral

8.6.5 In recommendation 106 I propose that provision be made for the deferral of complaints in certain limited circumstances. If this recommendation is adopted then it will be necessary to amend section 70(1) to provide that the Commissioner may defer a complaint.

Preliminary inquiries

8.6.6 Section 70 anticipates only two alternative courses of action when I receive a complaint - to investigate the complaint or to take no action. In fact, I receive a number of complaints for which neither course of action is immediately appropriate and instead I make preliminary inquiries of the complainant. It is undesirable that section 70 should ignore this third appropriate course of action since at present it does not accurately describe the appropriate range of

¹³ Human Rights Act 1993, section 76(3).

¹⁴ Ombudsmen Act 1975, section 17(3).

¹⁵ In passing, while there may be no good reason to require the Commissioner to tell the respondent in all cases of the grounds for which he is deciding to take no action, or no further action, obviously it is necessary that notification be given to the respondent where the Commissioner decides to take no further action. Such notification is given under section 75.

“Complaints should only be lodged by those directly affected (or their agents acting on their behalf). Given the Privacy Commissioner’s discretion to investigate on his or her own motion, there is no need to permit persons *other* than those affected (ie the officious bystander) to lodge complaints.”

- TELECOM NEW ZEALAND,

SUBMISSION UV13

action to be taken on receipt of a complaint. Where I make preliminary inquiries at present, I reconcile my actions with section 70 by taking the position that the inquiries are necessary to establish whether indeed I have a “complaint”, that is a complaint within jurisdiction. If I do not then, in a sense, section 70 does not apply. If I do, then I will indeed take one of the two courses of action mentioned in section 70 as soon as those preliminary inquiries are complete.

- 8.6.7 Typical preliminary inquiries of a complainant include:
- establishing whether a complaint really falls within my jurisdiction - which is not always plain from the initial communication;
 - asking for details of the respondent without which an investigation cannot commence anyway;
 - establishing for certain that the complainant does wish the matter to be investigated and is not simply raising a matter of concern for my information or to receive advice on the application of the law.
- 8.6.8 There are a number of complaints which, although within jurisdiction, are unlikely to succeed because of a relevant provision in the Act or a consistent line of interpretation on similar cases. For example, a complainant may not be aware that a respondent could rely upon the domestic affairs exemption in section 56 or that the case is similar to one in which the withholding of information was upheld by the Tribunal.
- 8.6.9 The approach that I have tended to take where a complaint appears to be beyond my jurisdiction is to explain that I will not take the matter further unless the complainant responds and answers the jurisdictional problem. No further action is taken unless the complainant comes back to me. In cases where the complaint is within jurisdiction, but there is an apparent answer in a section of the Act or in a precedent case, I explain to the complainant that unless I hear again I will presume that he or she does not desire that action be taken on the complaint. If I do not hear back, I write again to the complainant after a reasonable period communicating my decision to take no action on the complaint pursuant to section 71(1)(d).
- 8.6.10 I suggest that a provision should be inserted in the Act reflecting that such preliminary inquiries do appropriately occur. A precedent is to be found in section 42 of the Australian Privacy Act which states:
- “Preliminary inquiries**
Where a complaint has been made to the Commissioner, the Commissioner may, for the purpose of determining:
(a) whether the Commissioner has power to investigate the matter to which the complaint relates; or
(b) whether the Commissioner may, in his or her discretion, decide not to investigate the matter;
make inquiries of the respondent.”¹⁶
- 8.6.11 A provision dealing with preliminary inquiries could be incorporated into section 70 or established as its own section. Rather than specify the provision as a third option in addition to the two alternatives set out in section 70(1) I suggest that it be drafted as allowing the notification to the respondent to be postponed until preliminary inquiries are undertaken. In this fashion, once the preliminary inquiries are made the Commissioner may still simply choose one of the two alternatives in section 70(1) for a complaint which appears within jurisdiction.

¹⁶ Privacy Act 1988 (Australia), section 42. In the situation I am outlining the preliminary inquiries would be made of the *complainant*.

**RECOMMENDATION 104**

Section 70 should be amended to recognise that a decision to investigate a complaint, or to take no action on a complaint, may be postponed until preliminary inquiries are made of the complainant for the purpose of determining whether:

- (a) the Commissioner has power to investigate the matter; or**
- (b) the Commissioner may, in his or her discretion, decide not to investigate the matter; or**
- (c) the complainant wishes to proceed with the complaint.**

Complaints beyond jurisdiction

8.6.12 Complaints which are beyond jurisdiction pose a particular problem. From the way that Part VIII is presently drafted it seems that such communications are not to be treated as “actions that appear to be an interference with privacy” which is my function under the Part by virtue of section 69. For example, the grounds upon which the Commissioner may decide to take no action on a complaint under section 71 omit any reference to the fact that a complaint does not constitute an interference with the privacy of an individual. The Australian Privacy Act has that as the first reason for which the Commissioner may decide not to investigate or to investigate further a complaint.¹⁷

8.6.13 It appears to be intended that where a communication in the nature of a complaint is made to the Commissioner which is beyond jurisdiction that the formal complaints processes are not to be followed and, for example, cannot progress to the Tribunal. Although the Act is silent, good public administration would have me notify the person explaining that I have no jurisdiction to investigate the matter. That would not amount to a decision under section 71. However, it would amount to the exercise of a statutory power of decision that could be judicially reviewed. If this is the intended process it may be desirable for aspects of it to be explicitly set out in Part VIII.

8.6.14 However, consideration could be given instead to allowing the Commissioner to make a determination that the complaint appears to be beyond jurisdiction and to allow that matter solely (and not the substance of the complaint) to be the subject of Tribunal proceedings at the suit of the aggrieved individual. This may be an appropriate way of dealing with these issues since otherwise my view on the jurisdictional question would appear to be a bar to taking matters to the Tribunal whereas normally I simply render opinions which can, if proceedings are taken, be substituted by the opinion of the Tribunal. I might add that this course has actually been taken in proceedings before the Tribunal although the jurisdiction might be open to question.¹⁸ Consideration might also have to be given, for consistency, to the position of decisions concerning transfer under sections 72 to 72B of the Act.

**RECOMMENDATION 105**

Consideration should be given to establishing a process whereby a decision by the Commissioner that a complaint is beyond jurisdiction can, on this question alone, be referred by the complainant to the Complaints Review Tribunal for its decision on the matter.

8.7 SECTION 71 - Commissioner may decide to take no action on complaint

8.7.1 This section sets out the various grounds upon which I may, in my discretion, decide to take no action, or no further action, on a complaint.

8.7.2 Seven specific reasons are listed in respect of which I may decide to take no

¹⁷ Privacy Act 1988 (Australia), section 41(1)(a).

¹⁸ See *Laing v Complaints Assessment Committee*, Complaints Review Tribunal, CRT decision No 9/98, 22 June 1998.

“The Commissioner should not be empowered to take no action at all upon a complaint. The Commissioner should take some action - perhaps initiate an investigation - before reaching the conclusion that no further action should be taken.”

- TVNZ, SUBMISSION UV10

action on a complaint. Those are the only such reasons I may rely upon. However, in addition to those seven reasons, I may decide to take no *further* action on a complaint which I have started investigating for a further broader reason set out in section 71(2). That allows me to take no further action on a complaint if it appears to me that having regard to all of the circumstances of the case any further action is unnecessary or inappropriate.

8.7.3 I have carefully examined this section to see if there is any potential to appropriately screen out any further complaints given that my resources are fully stretched with the present complaints workload.¹⁹ My discretion to discontinue is satisfactory, from my point of view, where an investigation has already commenced. The specific provisions in subsection (1) and the general provision in subsection (2) provide me with all of the discretion that I believe I need. However, if the discretion to take no action is to contribute to diminishing the complaints queue, in some small fashion, it would need to be directed towards complaints for which no investigation has begun. The discretion to take no action on complaints without investigation is, quite rightly, tightly circumscribed since the meritorious complaints might be affected as well as the unmeritorious.

8.7.4 In fact, discontinuance on complaints where no investigation has been commenced is a double-edged sword for complainants and respondents. While it may be a blow to a complainant to hear that his or her complaint will not be investigated at all, the determination under section 71 also thereby permits him or her to take the matter directly to the Tribunal.²⁰ Similarly, from the perspective of the agency any initial euphoria at a potential complaint being “killed” may be tempered by the realisation that the complainant may take the matter to the Tribunal and the matter will not have benefited from the attempts by the Privacy Commissioner to look into the facts and sort the matter out in a conciliatory fashion.

Deferral of complaints

8.7.5 The grounds for taking no action on a complaint are appropriate. However, I have concluded that the Act would be enhanced through a provision allowing for the “deferral” of a complaint until a complainant has taken a particular action. “Deferral” would be a new category standing between investigation of a complaint and a decision to take no action.

8.7.6 The following features of the proposal should be noted:

- a decision by the Commissioner to defer a complaint would not entitle the aggrieved individual to take proceedings on the complaint to the Complaints Review Tribunal;
- the complaint would remain “on the books” of the Privacy Commissioner but no action would be taken on it except notification to the complainant explaining that investigation had been deferred until the individual had taken the requisite action (either taking the complaint up directly with the agency or with a recognised industry complaints body);
- a deferred complaint would not be queued in the Commissioner’s system until it ceases to be in a state of deferral - providing an incentive for individuals to make early efforts to seek to sort matters out for themselves if they can;
- deferral would *not* be automatic for all complaints that have not been taken up with an agency or recognised industry complaints body - the Commissioner would only use the deferral power where it appeared reasonable for the complainant to take the requisite action - in certain complaints the in-

¹⁹ At present the queue for complaints to be investigated is approximately 12 months from the date that the complaint is received - and this queue is growing. See Appendix J.

²⁰ Privacy Act, section 83.

“A complaints procedure is clearly the most accessible and barrier free approach to seeking redress. The trade-off for such an open mechanism is that screening out of insubstantial complaints is difficult and resource intensive. In comparison the cost and procedural barriers of litigation in the general courts usually provides a filter that prevents frivolous grievances progressing further, but at the same time may prevent deserving complainants from seeking redress.”

- MINISTRY OF JUSTICE,
SUBMISSION UV15

dustry body may be an inappropriate arbitrator of certain privacy disputes and on some occasions further direct contact between complainant and respondent may lead to more polarised positions which might hamper, rather than expedite, a resolution of the matter.

- 8.7.7 Neither the notion of “deferral” nor the placing of obligations on complainants to take matters up directly with respondents are entirely new for privacy laws. Section 41(3) of the Australian Privacy Act allows their Commissioner to defer the investigation of complaints in certain circumstances. The Australian Commissioner also has the power not to investigate a complaint where satisfied that:

“although a complaint has been made to the Commissioner about the Act or practice, the complainant has not complained to the respondent.”²¹

- 8.7.8 A further example of deferral is to be found in the Personal Health Information Act 1997 (Manitoba) which provides:

“The Ombudsmen may decide not to investigate a complaint about access or may defer investigating it if:

- (a) the complaint concerns a health care facility or health services agency and there is an internal appeal procedure that the complainant has not used; or
- (b) the complaint concerns a health professional and there is an expeditious and formal procedure for addressing such complaints available through a body that has statutory responsibility for regulating the practice of the health professional, which the complainant has not used.”²²

- 8.7.9 The proposal would introduce the notion of deferring a complaint. It would need to be made clear that a decision to defer did not entitle an individual to take the substantive complaint to the Tribunal. A deferral would not affect an individual’s right to take a complaint directly to a court in circumstances where that would be permitted under section 11(1). The new provision may have to spell out some matters such as the length of time that a complaint may be deferred and whether it lapses at that point.

Grounds for deferral

- 8.7.10 The first proposed ground for deferral is where the complainant has not complained to the respondent. This is relatively straightforward and I would desire that the resultant clause keep matters relatively simple. An elaborate procedure is not needed. I would simply expect the complainant to put him or herself in the position of most other complainants. The complainant would probably telephone the agency, or write a letter to it, and if still unable to resolve the complaint will revert to my office with a copy of the agency’s reply, an account of the conversation held or a copy of the letter written and the fact that no reply has been received.
- 8.7.11 The second proposed ground has some similarities to the existing sections 71(1)(f)(i) and (g). That is, that the complaint may be deferred where there is an industry complaints mechanism that the Commissioner considers ought to be utilised. Suitable criteria for recognition could be prepared or I might have re-

²¹ Privacy Act 1988 (Australia), section 41(1)(b). That ground is not appropriate to directly incorporate into section 71(1) of our Act because that decision itself may allow the complainant to take the matter to the Tribunal. No such implication flows from the Australian Commissioner’s decision not to investigate since there is no Tribunal under the Australian Act.

²² Personal Health Information Act 1997 (Manitoba), section 41(2).

“Providing the Privacy Commissioner with the discretion not to take up a complaint until such time as all reasonable attempts have been made by the individual to resolve the issue could ensure that only cases with substance can proceed to the Commissioner or courts.”

- INLAND REVENUE DEPARTMENT,
SUBMISSION UV7

gard to existing standards for the adequacy of complaints mechanisms.²³ There are no independent complaints mechanisms which would have *all* of the qualities that I would think necessary to substitute adequately for the Act's complaints mechanism. However, some exist which would be suitable for *some* complaints.

8.7.12 The two most promising mechanisms, the Banking Ombudsman and the Insurance and Savings Ombudsman, have a number of excellent features providing for professional investigation, impartial adjudication, and the awarding of consumer remedies.²⁴ However, their jurisdiction is based upon concepts and issues specific to the industries and not, for example, to address alleged interferences with privacy of individuals, or breaches of the information privacy principles. Another problem with industry complaints bodies is that they may have limited power to obtain evidence where that concerns someone else who will not consent to its release.

8.7.13 Furthermore, the compensation that can be awarded is not commensurate with that available under the Act. Nonetheless, since many cases involve compensation at the lower end of the scale they may each be adequate for many relevant privacy cases. Indeed, even under existing provisions my office often encourages some complainants to take their matters up with those industry ombudsmen.

8.7.14 While the two ombudsmen mentioned are the main industry bodies I would have in mind, others may exist or be created from time to time which may be suitable to address a deferred complaint in circumstances where I would not generally be willing to exercise a decision to take no action under section 71(1)(g). Where I defer on this ground I anticipate that I would notify the complainant and indicate the steps to be taken - namely to complain to the specified complaints body. The notification would also indicate at which point the complainant could ask the matter to be again taken up by me. This may involve, for example, an industry ombudsman rendering an opinion that a complaint cannot be settled or falls outside his or her jurisdiction.

8.7.15 Although I have made my recommendation in the context of section 71 it is likely that the amendment to give effect to the proposal would affect other sections as well. For example, section 70 would need to be amended. Parliamentary Counsel may have a view as to whether the provisions for deferral should appear in section 70, section 71 or constitute their own intermediate section.

8.7.16 While I see the introduction of deferral as a useful reform, no-one should be under any illusion that it will significantly reduce the complaints queue. It may contribute to a small reduction, to be welcomed, but the proposal is really directed to enhancing the processing and prioritising of complaints investigation whether or not there is a backlog of complaints.



RECOMMENDATION 106

Provision should be made in Part VIII of the Act for the Commissioner to defer action, or further action, on a complaint where:

- (a) the complainant has not complained to the agency concerned and the Commissioner considers that the complainant should do so in an attempt to directly resolve the matter; or**
- (b) the complaint concerns an agency in respect of which there is an independent, expeditious and appropriate procedure for addressing such complaints available through an industry body which the complainant has not used.**

²³ For example, see the Australian Federal Bureau of Consumer Affairs, "Benchmarks for Industry-based Customer Dispute Resolution Schemes", November 1996, set out in Office of the Retirement Commissioner, *Review of Banking and Savings Ombudsman Schemes and Consideration of the Need for a Statutory Savings Ombudsman*, July 1997, Appendix I.

²⁴ Indeed, to be entitled to use the title "Ombudsman" the credibility of the process must be established to the satisfaction of the Chief Ombudsman. See Ombudsmen Act 1975, section 28A.

"While it is possible for a large organisation, such as a bank, to provide internal complaints procedures of the kind described, it is clearly impractical to expect the same of smaller agencies. Because I have seen a number of cases where the initial problem has been exacerbated by the poor handling of the complaint, I do not think it desirable that complainants should routinely be required to approach agencies, or should have their complaints forwarded to agencies, for attempts at resolution unless the Privacy Commissioner is satisfied that the agency in question has appropriate procedures for complaints handling."

- BANKING OMBUDSMAN,
SUBMISSION UV14

Limitation period

8.7.17 The first ground upon which I may decide to take no action, or no further action, on a complaint is where, in my opinion:

“The length of time that has elapsed between the date when the subject matter of the complaint arose and the date when the complaint was made is such that an investigation of the complaint is no longer practicable or desirable”.²⁵

8.7.18 It should come as no surprise that I have rarely taken a decision based upon this ground, given the fact that the complaints jurisdiction is relatively young. The Privacy Act only applies to actions which have occurred on or after 1 July 1993.²⁶ I have not yet found any significant problem of individuals bringing complaints to me a long time after the subject matter of the complaint. Were that to happen section 71(1)(a) provides an adequate filter for my purposes. As a backstop, pursuant to section 4(1)(d) of the Limitation Act 1950, any proceedings would generally be barred after the expiration of six years from the date on which the cause of action accrued.

8.7.19 I do not recommend any change to the limitation period at this stage. It is a matter which could be reviewed in later years when the complaints jurisdiction has matured if problems arise.

8.7.20 However, I should observe in this context that my own complaints queue now extends to more than 12 months.²⁷ This is not the fault of individual complainants but it may, in fact, mean that the investigation of some complaints may be no longer practicable or desirable given the length of time that has elapsed between the date when the subject matter of the complaint arose *and the date upon which it is practicable for the Commissioner to investigate*. This is a sorry state of affairs which has the potential to seriously impact on some complainants and cause inconvenience and irritation to some agencies when called upon to explain their actions many months after the relevant actions occurred. These problems cannot be solved by a shorter limitation period but instead point to the need to devote further resources to enabling complaint investigations to be completed with appropriate despatch.

8.8 SECTION 72 - Referral of complaint to Ombudsman

8.8.1 Section 72 requires me to consult the Chief Ombudsman where I receive a complaint which more properly relates to an area under the Ombudsmen’s jurisdiction. There are not many of these. Section 17A of the Ombudsmen Act imposes a corresponding duty on the Ombudsmen under which there is a frequent transfer of complaints. The provision has operated satisfactorily in practice.

8.9 SECTION 72A - Referral of complaint to Health and Disability Commissioner

8.9.1 I must consult with the Health and Disability Commissioner where I receive a complaint that more properly relates to an area under the Health and Disability Commissioner’s jurisdiction. Section 40 of the Health and Disability Commissioner Act imposes a corresponding duty on the other Commissioner. There are not as many complaints transferred pursuant to this provision as to the Ombudsmen.

²⁵ Privacy Act, section 71(1)(a).

²⁶ Furthermore, breaches of certain principles occurring before 1 July 1996 have not been able to be taken to the Tribunal - Privacy Act, section 79.

²⁷ See Appendix J.

8.10 SECTION 72B - Referral of complaint to Inspector-General of Security and Intelligence

- 8.10.1 Section 72B requires me to consult the Inspector-General of Intelligence and Security where I receive a complaint that more properly relates to an area under his jurisdiction. The section provides for the transfer of appropriate cases but, thus far, there have been no such consultations or transfers.
- 8.10.2 When the Privacy Act was enacted there was a single provision for the referral of complaints (section 72 allowing for transfer to the Ombudsman). With the creation of the Health and Disability Commissioner and Inspector-General of Intelligence and Security there are now three such provisions. Conceivably further provisions might be needed in the future if relevant complaints bodies are established. There may even be a case for existing complaints bodies to be referred to such as the Police Complaints Authority, Human Rights Commission and the Broadcasting Standards Authority. I note that the Health and Disability Commissioner Act and the Inspector-General of Intelligence and Security Act, both of which were passed later than the Privacy Act, have single combined complaints transfer provisions. In an effort to streamline the Privacy Act, and to create a simpler framework for the addition of any further complaints transfer provisions, sections 72, 72A and 72B should be combined into a single section and consideration be given to adding other statutory complaints bodies. If necessary, a new schedule could be created.



RECOMMENDATION 107

Sections 72, 72A and 72B should be combined into a single section providing for the referral of complaints to the Ombudsmen, Health and Disability Commissioner and Inspector-General of Intelligence and Security, and consideration should be given to listing other statutory complaints bodies.

8.11 SECTION 73 - Proceedings of Commissioner

- 8.11.1 Section 73 requires the Commissioner to inform all interested parties of his or her intention to undertake an investigation and to inform the person to whom the investigation relates of the right to submit a written response to the complainant. I have observed elsewhere that the marginal note to this section is not particularly helpful and recommend that it be changed to “parties to be informed of investigation”.²⁸

8.12 SECTION 74 - Settlement of complaints

- 8.12.1 Section 74 provides that the Privacy Commissioner may endeavour to secure a settlement of the complaint without investigating it or investigating it further. It is plain from this section, and others, that Parliament intends that considerable emphasis be placed in my complaints processes upon seeking to secure settlements of complaints. It is important to understand this to obtain a full appreciation of the complaints processes in the Act. A significant role of the Commissioner is to try to sort out the privacy problems that have led individuals to become aggrieved at the actions of agencies and to do so in a fashion which resolves those problems, if appropriate compensates the aggrieved individual and seeks to obtain assurance that the same breach of privacy is unlikely to occur again.
- 8.12.2 Quite often it becomes apparent fairly early in the piece that there really is “something” to the complaint and that while the investigation has not established all of the facts, or concluded the finer points of legal interpretation, the agency is partly at fault and ought to make some amends. Frequently I find

²⁸ See recommendation 2.



“Would enabling the complainant to go to the Complaints Review Tribunal result in any earlier investigation or merely shift the delay from one venue to another? Is it ultimately a matter of resources? If so, it is probably less costly to the community at large to increase the resources of the Privacy Commissioner.”

- NZ VIDEO DEALERS ASSOCIATION, SUBMISSION UV9

that all a complainant really wishes to secure is an apology, some out of pocket expenses, and an assurance from the agency that the same thing will not happen again. Often complainants say that they want to make sure that what happened to them could not happen again to someone else.

- 8.12.3 If a settlement can be secured in those circumstances, and I can be satisfied that the agency is taking steps to ensure that a breach is not repeated, it will frequently be unnecessary to go on with an investigation.

8.13 SECTION 75 - Parties to be informed of result of investigation

- 8.13.1 This provides that I must conduct my investigations “with due expedition” and at the end of the investigation am required to inform the parties concerned of the results and of what further action (if any) I propose to take in respect of the complaint.

- 8.13.2 I do not have the resources necessary to process all of the complaints that are received within time-frames that I believe New Zealanders would expect as reasonable. I do not believe that Parliament intended, when it enacted the Privacy Act, that individuals should have to await 12 months before having their complaint investigated.²⁹

- 8.13.3 Such a situation was never allowed to exist when access reviews were the subject of review by the Office of the Ombudsmen. I believe that the Ombudsmen’s office is more appropriately funded and does a good job of processing its access reviews. However, I consider it quite unfair to my office, and more particularly for complainants and respondents, that a third party who might request information from a public sector agency will have their complaint about access to official information promptly investigated by the Ombudsmen’s office but their complaint about access to their personal information may languish for months. This is despite the fact that access requests by the individual concerned have always been seen as one of the most fundamental and important of the access rights established originally by the Official Information Act. Accountability is at the heart of freedom of information laws and it would seem that accountability for handling people’s personal information is now seen as less important. The fundamental nature, and importance, is manifest by the fact that:
- personal access rights to information held by public sector agencies are *legal rights* and not simply entitlements;
 - information may be withheld for fewer reasons because of the importance of the rights and no charge may be made for individual access to such information.

- 8.13.4 I am in breach of the requirement of this section to conduct investigations “with due expedition” if the investigation is to be timed from the date upon which I receive a complaint. Through the queuing system I have endeavoured to ensure that my staff are not overwhelmed with too many current files. Complainants get an unrealistic impression that a complaint can then be investigated “with due expedition”. Therefore once a complaint file is allocated I do expect my staff to handle the work efficiently and expeditiously. However, it is of little comfort to complainant and respondent to know that in due course when the complaint reaches the front of the queue it may then be handled with due expedition.

- 8.13.5 It is anomalous that a third party such as a journalist may have a refusal to make available information about a person investigated promptly while the individual concerned who is refused access to their own information cannot get that review without a long delay.

“The use of Commissioners and Ombudsmen is considerably cheaper than the Courts. We consider that more resources should be made available to enable the Office of the Privacy Commissioner to promptly facilitate settlement of disputes.”

- NZ GENERAL PRACTITIONERS’ ASSOCIATION, SUBMISSION S28

29 Details of the complaints queue are set out as at Appendix J.

**RECOMMENDATION 108**

Adequate funding should be made available so that the volume of complaints received at the Office of the Privacy Commissioner can be processed, as required by section 75, “with due expedition”.

8.14 SECTION 76 - Compulsory conferences

8.14.1 This section provides for the calling of compulsory conferences enforceable by summons. The provision is derived from similar provisions in the Protection of Personal and Property Rights Act 1988 relating to compulsory pre-hearing conferences. Section 80 of the Human Rights Act 1993 makes similar provision but refers to the process as “compulsory conciliation” and the meeting as a “conciliation conference”. The Health and Disability Commissioner Act 1994, section 61, refers to it as a “mediation conference”.

8.14.2 I have used the power to call compulsory conferences very sparingly.

8.15 SECTION 77 - Procedure after investigation

8.15.1 Section 77 provides that after an investigation the Commissioner should attempt to secure a settlement of the matter and, where appropriate, obtain an assurance against repetition of the interference with privacy. Where a settlement and assurance cannot be secured, or where it appears that the action was done in contravention of a previous assurance, or that any term of a settlement has not been complied with, I may refer the matter to the Proceedings Commissioner for the purpose of deciding whether proceedings should be instituted before the Complaints Review Tribunal under section 82.

8.15.2 It may be desirable to make a small change to section 77(1)(a) to align it more closely to the approach for seeking settlement of complaints set out in section 74. Section 74 indicates that the Commissioner may use his best endeavours to secure a settlement “where it appears possible to secure a settlement”. Section 77(1)(a) simply provides that the Commissioner “shall” use his best endeavours to secure a settlement where he is of the opinion that the complaint has substance. At some point the Commissioner has to conclude that attempts at settlement are fruitless through, say, the intransigence of the respondent or an unreasonable attitude of the complainant.

**RECOMMENDATION 109**

Section 77(1)(a) should be amended so that the Commissioner is required to continue endeavouring to secure a settlement only where it appears to the Commissioner that settlement is possible.

8.16 SECTION 78 - Procedure in relation to charging

8.16.1 Where a complaint is that a charge made for an information privacy request is unreasonable, the Privacy Commissioner, failing settlement, is to make a final and binding determination of the charge that ought reasonably to have been imposed.

8.16.2 When the Privacy of Information Bill was introduced it was proposed that no charge be made for giving access to information whether held in the public or private sectors. This would have continued the approach from the Official Information Act and extended it to the private sector as well. However, the Select Committee agreed with a variety of submissions that the making of a reasonable charge should be permitted for obtaining access to information held in the private sector. Consequently, there needed to be a procedure for complaints alleging that a charge levied was unreasonable. Mainstream complaints, if not amenable to settlement through the Commissioner’s processes, can be

“We are concerned at the large increase of complaints which your office is dealing with. Our experience of complaints about breaches of the Privacy Act or banker/customer confidentiality is that easy access to the free complaints investigation service provided by the Privacy Commissioner sometimes impedes the resolution of complaints. We believe that the Commissioner’s resources are better spent on the policy area ensuring that there is informed debate on what are increasingly complex issues.”

- WESTPACTRUST, SUBMISSION S34

taken to the Complaints Review Tribunal for determination. This was seen as undesirable for charging complaints and it was preferred that they be able to be determined without recourse to the Tribunal, which would have added time and cost to an issue which should be determined quickly and cheaply. Charging complaints under section 78 are the only ones for which the Commissioner may issue a final and binding determination.

- 8.16.3 The provision has worked satisfactorily and it would be inappropriate to have charging complaints able to be taken to the Tribunal. However, it may be appropriate to broaden section 78 so that it applies to all charging complaints not simply those alleging that a charge fixed in respect of an information privacy request is unreasonable. The section should perhaps also apply to complaints that the charge was made in circumstances where none at all was permissible, reasonable or not. The main circumstance in which this would arise is if a public sector agency made a charge notwithstanding the prohibition in section 35(1). The other circumstance is where a private sector agency makes a charge prohibited by a code of practice. Such complaints ought to be able to be determined in the same relatively straightforward manner as other section 78 complaints.



RECOMMENDATION 110

Section 78 should be broadened to encompass all charging complaints.

8.17 SECTION 79 - Breaches of certain principles occurring before 1 July 1996

- 8.17.1 Section 79 was part of the staged implementation of the Act. While all twelve of the information privacy principles were applied to agencies from “day one”, Tribunal remedies were not immediately available for all interferences with privacy. During the first three years I could investigate complaints concerning breaches of any of the principles but if I was unable to secure a settlement then proceedings could be taken to the Tribunal only if the complaint concerned principles 5, 6, 7 or 12.
- 8.17.2 The staged implementation did satisfactorily assist in the introduction of the Act. Had Tribunal remedies been fully available from the commencement of the Act I suspect that many agencies would have worried about their liability. With the three year “breathing space” agencies had the opportunity to modify their information handling practices before enforceable sanctions became available. The period also gave the opportunity for professional associations and trade bodies to give advice to their membership as to compliance and for my office to undertake training and education activities. The complaints that were investigated during the early years were done so on an Ombudsman-type basis (that is, without prospect of an enforceable remedy) and some of the resultant opinions were disseminated through the issue of case notes. A number of settlements were achieved involving the payment of damages.
- 8.17.3 The staged introduction was not a complete success in all respects since it allowed a degree of complacency to be established in some quarters particularly with respect to the collection principles. Some advisers misunderstood the implementation arrangements and thought that eight of the twelve principles did not apply until 1996 - whereas they had applied since 1993. This was an unfortunate message since a pro-active attention to information collection practices almost inevitably leads to fewer compliance problems down the track with use and disclosure of information. Another consequence related to the fact that Tribunal precedents were largely unavailable for the first three years. Indeed, there was only a single decision of the Tribunal in 1994 and one interim decision in 1995. From 1996 onwards, with the completion of the transitional arrangements, a modest but steady stream of Tribunal decisions have been rendered providing the guidance on the interpretation of the Act.

8.18 SECTION 80 - Commissioner to report breach of duty or misconduct

- 8.18.1 This section requires me to refer evidence of any significant breach of duty or misconduct on the part of an agency or an officer or employee or member of an agency to the appropriate authority.
- 8.18.2 Generally speaking, my complaints and investigation role is to find out if an interference with privacy has occurred and, if so, to see if the complaint can be settled with steps taken to avoid future breach. My primary focus is on the effect on privacy, both in the present case and the potential for harm to privacy in similar circumstances in the future. However, in the course of investigations it sometimes transpires that the action that constituted the interference with privacy also amounts to a significant breach of duty or misconduct. Occasionally, the breach of duty or misconduct is not actually the interference with privacy itself but has simply been turned up during the investigation.
- 8.18.3 I do not commonly refer matters to other authorities. However, during the period under review I utilised the provision in the following ways:
- referring the failure of a professional person to respond to my requirements to the appropriate professional association;
 - referring a case of breach of the Private Investigators and Security Guards Act to the registrar under that legislation;
 - referring the actions of an official to the relevant Minister;
 - referring the actions of an individual to the Police.
- 8.18.4 It should be noted that section 80 imposes on me a *mandatory* duty to report significant breach of duty or misconduct. I am not, for example, to be swayed from doing so by the fact that an agency, or an employee, is able to reach a satisfactory settlement with a particular complainant. I am not open to negotiation with respondents (or indeed complainants since surprisingly the misconduct that is exposed is not always on a respondent's part) as to the question of whether misconduct is to be reported.

8.19 SECTION 81 - Special procedure relating to intelligence organisations

- 8.19.1 A special procedure is established where a complaint is lodged against an intelligence organisation, that is the NZ Security Intelligence Service (NZSIS) or the Government Communication Security Bureau (GCSB). This special procedure was not in the Privacy of Information Bill when introduced but was inserted by the Select Committee after taking submissions. Unfortunately, a drafting error crept into the process with the provision, and the heading, referring to “intelligence agencies” rather than the term defined in section 2, “intelligence organisations”. Section 81 was repealed and substituted by section 4 of the Privacy Amendment Act 1996 and was deemed to have taken effect on 1 July 1993. This resolved the problem.
- 8.19.2 At present section 57 provides that only principles 6, 7 and 12 apply to intelligence organisations. Elsewhere in this report I have recommended that several additional principles should be applied.³⁰ The special procedure for complaints against intelligence organisations prevents matters being taken to the Complaints Review Tribunal and therefore public hearings and enforceable orders do not feature as part of the process. Instead, consistent with the needs of national security, a process is provided whereby if complaints cannot be settled with the intelligence organisation a report is made to the Prime Minister which may be laid before Parliament.

³⁰ See recommendation 83.

- 8.19.3 To date there have been no complaints against GCSB. There have been a number relating to the NZSIS involving requests for access to personal information which have been refused. To date no reports have been made to the Prime Minister and therefore a full opportunity to review the special procedure and practice is not yet possible.
- 8.19.4 Since the special procedure was created there have been two related developments. These are the enactment of the Intelligence and Security Committee Act 1996 and the Inspector-General of Intelligence and Security Act 1996. The role of the Inspector-General of Intelligence and Security is mentioned elsewhere in this report.³¹ The Intelligence and Security Committee is a statutory committee of senior members of Parliament which has amongst its functions:
- to examine the policy and administration of an intelligence organisation; and
 - to consider any matter referred to the Committee by the Prime Minister by reason of that matter’s security or intelligence implications.³²
- 8.19.5 The functions of the Committee do not include originating or conducting enquiries into complaints by individuals concerning the activities of an intelligence organisation that are capable of being resolved under any other enactment.³³ It seems to me that there might be a purpose in providing for reports to the Prime Minister under section 81 to be referred to the Committee on occasion. Such referral would not be intended as part of the resolution of the complaint which, if it has reached the stage of a report to the Prime Minister, is a matter for the Prime Minister, but rather because of the possible relevance to questions of the policy and administration of an intelligence organisation. This might be valuable where, for example, an intelligence organisation might seek to adopt a standard policy in respect of a broad class of complaints. Referral of the report to the Committee should not be seen as a substitute for tabling the report in Parliament (in whole or part) in appropriate cases. It seems to me that laying the report before Parliament, or referring it to the Committee, have separate purposes and either or both might be followed in particular cases.
- 8.19.6 I do not consider that amendment is essential since there would appear to be sufficient discretion under the Intelligence and Security Committee Act for the Prime Minister to take the initiative to forward the report without any further statutory authority. It is also the case that section 81 is primarily directed towards complaints investigation and resolution and the step that I am proposing is only indirectly related to that and, in fact, more relevant to the general policy and administration for complaints of such a type. However, since this is the first opportunity for the matter to be considered since the enactment of the two 1996 Acts I make a recommendation that the change may be examined.



RECOMMENDATION 111

Consideration should be given to including in, or following, section 81(5) a provision that the Prime Minister may refer a report given under section 81(4) to the Intelligence and Security Committee.

8.20 SECTION 82 - Proceedings before Complaints Review Tribunal

“Specialist” tribunal

- 8.20.1 Section 82 introduces the Complaints Review Tribunal. This, and the following 7 sections, govern proceedings before the Tribunal which is utilised for proceedings under the Privacy Act, Human Rights Act, and Health and Dis-

³¹ See paragraphs 6.13.25 - 6.13.30.

³² Intelligence and Security Committee Act 1996, section 6(1)(a) and (d).

³³ Intelligence and Security Committee Act 1996, section 6(2)(c).

VIII

s 82

285



**Susan Bathgate: Current
Chairperson of the Complaints
Review Tribunal.**

PHOTO: S BATHGATE

ability Commissioner Act. The Tribunal occupies an important place in the enforcement scheme of the Act. A credible complaints system needs a way of issuing final and binding rulings where a matter cannot be resolved through investigation, conciliation and an independent recommendation. By vesting powers of determination in a judicial tribunal it has been possible to avoid creating a scheme where such powers might be vested in the Commissioner. While the Commissioner is seized of a complaint, the most that he can do is investigate, seek to settle a complaint, and if necessary issue a formal opinion which has persuasive value but is not binding.

- 8.20.2 The Complaints Review Tribunal deals with complaints by individuals of a breach of their human rights. It had existed for many years previously under the title of Equal Opportunities Tribunal where its jurisdiction extended solely to complaints made under the Human Rights Commission Act 1977, which involved allegations of discrimination or sexual harassment. Its jurisdiction now also includes, in addition to privacy, complaints of a breach of the Code of Health and Disability Services Consumers' Rights. Accordingly, it is not a specialist *privacy* tribunal but rather a specialist human rights or complaints tribunal.
- 8.20.3 While the need for a judicial body to have the role that the Tribunal presently serves is accepted, it might be questioned whether the District Court might fulfil the role adequately. The discussion paper asked the question of whether the existing role of the Tribunal should be transferred to the District Court. Fourteen submissions were made opposing any transfer³⁴ and none supported the proposal. Two submissions, while not offering support or opposition, offered further comments such as a suggestion that complainants be given the right to elect whether they take proceedings to the Tribunal or District Court.³⁵
- 8.20.4 Many of the submissions favoured perceived greater flexibility, speed and lower cost of tribunal proceedings as against the District Court. A tribunal is also seen as less daunting for unrepresented plaintiffs and respondents compared with a court. I take the view that there is no case for change at present but believe that the matter should be looked at again at the time of the next review. While the specialist tribunal model is a good one, it may be that at some point in the future when the Act has been "bedded in" over a number of years that efficiencies could be gained through placing the functions with the District Court. While as yet premature, there may in the longer term be positive benefits in bringing the jurisdiction into the mainstream of legal proceedings. Provision could be made for a District Court Judge to sit with assessors if that would assist. Initially there would be advantages in a limited number of judges exercising the jurisdiction to build up experience, knowledge and consistency.
- 8.20.5 I believe that the panel from which the Tribunal is made primarily consists of people who have experience in, or who would be able to contribute in respect of, proceedings brought under the Human Rights Act which has been the Tribunal's staple diet for many years. I am not aware of panel members being selected because of their knowledge of privacy issues. There may be some scope for further developing the Tribunal's expertise in privacy cases in the future through the selection of the panel. An alternative might be that if the Tribunal is chaired by a District Court Judge that Privacy Act cases could be heard solely before that person. Those proceedings should, I suggest, be able to be heard by the chairperson alone.

Section 82

- 8.20.6 Section 82 provides that the Proceedings Commissioner may take civil proceedings before the Complaints Review Tribunal against any person and in

³⁴ See submissions UV1-UV6, UV8-UV11, UV13, UV15, UV16 and S36.

³⁵ See submissions UV18 and S42.

“To allow a complaint to go straight to the Tribunal would cut out the conciliation/mediation stage and introduce from the outset, the litigious note which the Act’s authors attempted to discourage. It is doubtful if delays would be avoided; they would merely occur in a different context.”

- NZ EMPLOYERS FEDERATION,
SUBMISSION UV4

relation to an action of that person that is an interference with the privacy of an individual. The Proceedings Commissioner may also bring proceedings on behalf of an affected class of persons.

- 8.20.7 The Proceedings Commissioner is, like the Privacy Commissioner, a Human Rights Commissioner. The appointment is made pursuant to section 7(1)(d) of the Human Rights Act 1993. The involvement of the Proceedings Commissioner introduces a further independent element to review the strength of the evidence before commencing proceedings, and then to take the proceedings themselves. This is not a role that need be performed by the Privacy Commissioner and it has been seen as desirable in this, and similar contexts, to bring an independent person into the process.
- 8.20.8 The transitional provisions in section 79 have meant that cases which could go to the Tribunal have only started to build up since mid-1996. As it happens, the Proceedings Commissioner has not had a great deal of involvement in the taking of Privacy Act proceedings during the period under review as the cases that have gone to the Tribunal so far have all been taken by aggrieved individuals themselves where I have formed an opinion in favour of the respondent or have declined to refer the matter to the Proceedings Commissioner. For most meritorious cases, my office has usually been able to secure a satisfactory settlement of the complaint and an assurance that the interference with privacy will not be repeated. On only a small number of occasions have I referred matters to the Proceedings Commissioner to be taken to the Tribunal. Thus far, all such cases have been settled prior to the matter being heard before the Tribunal.
- 8.20.9 In cases brought by aggrieved individuals it is not necessary for the Proceedings Commissioner to become involved. Where he declines to appear the Privacy Commissioner may appear. I have adopted the practice to date of ensuring that I am represented before the Tribunal in pre-hearing conferences and in hearings before the Tribunal. In a developing jurisdiction such as this I have wished to use the opportunity to offer assistance to the Tribunal which might not otherwise be presented by the parties to a complaint. I believe that this practice has been of assistance to the Tribunal. Such an appearance does not constitute either Commissioner as a party enabled to appeal against the decision.
- Enforcement of assurances*
- 8.20.10 The inter-relationship of sections 74, 77, 82 and 85 does not seem ideal when it comes to making sure that assurances which are part of a settlement of a complaint are adhered to and if necessary enforced. Under sections 74 and 77 it is anticipated that satisfactory assurances will be obtained from respondents that repetition of any action that is the subject matter of the complaint will not be repeated. However, it is not made plain what will happen if such assurances are breached.
- 8.20.11 Assurances or settlements formally executed between the complainant and respondent might be enforced, irrespective of the mechanisms in the Privacy Act, as a contract. However, assurances obtained against repetition of the action, or similar action, are frequently not directed simply at actions affecting the individual complainant but, as a matter of public policy, to prevent further breaches of the Act affecting other individuals. Therefore, in some cases I have an interest on behalf of the public in ensuring that assurances are adhered to where the individual may not be so concerned. Indeed, assurances are a critical part of a complaints-based mechanism for securing broader compliance with the objectives of the Act. Without them, it is difficult to have confidence that individual complaints will indeed lead to a change in the prohibited behaviour.
- 8.20.12 It ought to be possible for the Proceedings Commissioner to take a case for a breach of an assurance given under sections 74 or 77. This could perhaps be

“The Ministry acknowledges the considerable resource pressures placed on the complaint investigation process. It also notes that to date few privacy complaints have been referred to the Tribunal. The involvement of the Commissioner prior to Tribunal proceedings serves the invaluable function of clarifying the nature of the complaint, particularly the issues in dispute. It is also likely that complaints of a less substantive nature and ones which are capable of resolution by a more conciliatory means, could end up in the CRT.”

- MINISTRY OF JUSTICE
SUBMISSION UV15

secured by an amendment to section 82(2) simply adding the words “or which is a breach of an assurance given to the Privacy Commissioner under section 74 or 77”. In addition to this, there may need to be an amendment to section 85 to make clear the powers of the Tribunal to grant the listed remedies not only where there has been an “interference” but also where there has been a breach of an assurance. There may well be other or better ways to achieve a similar effect.

- 8.20.13 A comparable problem has arisen in relation to settlements obtained under the Human Rights Act complaints processes. In *Proceedings Commissioner v Ah Voo*³⁶ the Complaints Review Tribunal held that there was no jurisdiction under section 83 of the Human Rights Act for the Proceedings Commissioner to enforce a settlement made pursuant to section 81. The Tribunal said:

“We think that the absence of the power to enforce settlements is probably an unfortunately omission of the Act. It is difficult to accept that the legislature intended this Tribunal to hear and determine proceedings concerned with breaches of the Act but not those concerned with enforcing settlements made pursuant to the Act.”

A similar sentiment might apply in respect of assurances given under the Privacy Act.



RECOMMENDATION 112

Provision should be made by amending section 82(2), or otherwise, to allow Tribunal proceedings to be brought by the Proceedings Commissioner where there is a breach of an assurance given to the Privacy Commissioner under section 74 or 77.

8.21 SECTION 83 - Aggrieved individual may bring proceedings before Complaints Review Tribunal

- 8.21.1 Section 83 provides for individuals to bring proceedings before the Tribunal where the Privacy Commissioner or Proceedings Commissioner is of the opinion that the complaint does not have substance, or should not be proceeded with, or, where the Proceedings Commissioner would be entitled to bring proceedings, he or she agrees to that individual bringing the proceedings or declines to bring proceedings. By allowing aggrieved individuals to undertake proceedings before the Tribunal themselves, the Act provides individuals with an alternative to having to make an application for judicial review against the Privacy Commissioner or Proceedings Commissioner, as well as obviating the need for wider litigation.

- 8.21.2 A number of complainants have pursued proceedings to the Tribunal with varying degrees of success. The statutory scheme makes clear that the Privacy Commissioner’s opinion is not necessarily the last word - this is the prerogative of the Complaints Review Tribunal.³⁷

- 8.21.3 Interestingly, all of the decisions issued to date have related to proceedings brought by individuals and not by the Proceedings Commissioner. This is not a trend that concerns me since I believe it largely reflects a high degree of success with settling most complaints without the need for Tribunal proceedings. It also reflects my view that where reasonable efforts to settle are made but declined by the aggrieved individual, it is appropriate for the litigation to be undertaken by that person. If no reasonable offer is made and the circumstances justify, I will refer the complaint. It is important that recalcitrant respondents know that that can

³⁶ 15 December 1997, CRT 17/97.

³⁷ Or perhaps, depending upon one’s perspective, the courts if an appeal is taken on a point of law.



“Complaints procedures and enforcement are an integral part of the Privacy Act. A complainant should be able to select from as wide a range of complaint avenues as possible.”

- FINANCE SECTOR UNION,
SUBMISSION UV1

“The complainant should be given the right to go to the Complaints Review Tribunal if the Commissioner has not made a determination within 6 months of the complaint being lodged.”

- AUCKLAND DISTRICT COUNCIL OF
SOCIAL SERVICE, SUBMISSION UV12

occur. It also reflects the implementation provisions whereby until mid-1996 most complaints could not be taken to the Tribunal. I believe that a more realistic position in respect of the ratio of individually-brought cases to Proceedings Commissioner cases will only become apparent in a few years from now. I do expect a number of cases referred to the Proceedings Commissioner will, from time to time, go to the Tribunal for adjudication.

8.22 SECTION 84 - Remedies that may be sought

8.22.1 Section 84 provides that there are no restrictions on the remedies that may be sought by the Proceedings Commissioner or the aggrieved individual from among those described in section 85.

8.23 SECTION 85 - Powers of Complaints Review Tribunal

8.23.1 This section sets out the remedies that the Tribunal may grant if it finds, on the balance of probabilities, that an action is an interference of the privacy of an individual. The Tribunal is able to grant:

- declarations;
- restraining orders;
- compensatory damages;
- orders specifying acts the defendant must perform to remedy the interference;
- any other relief that the Tribunal thinks fit

8.23.2 The Tribunal may also award costs against either party. Costs ought not to be automatically regarded as following the event in respect of proceedings concerning the withholding of personal information in response to an access request. While costs may well be appropriate to be visited upon recalcitrant agencies which have delayed matters, and caused costs to be borne by the complainant, there will be many cases where the agency has withheld information believing it to be justified in the circumstances by reason of an apparently applicable withholding ground. For example, an agency might withhold information to protect the privacy of another person. Any kind of signal that costs may automatically follow the event would undesirably encourage agencies to avoid the risk by releasing the information regardless of qualms regarding the privacy of the other person. Costs need to be considered on a case by case basis if the competing needs of privacy are to be fairly addressed.

8.24 SECTION 86 - Right of Proceedings Commissioner to appear in proceedings

8.24.1 Section 86 provides for the appearance of the Proceedings Commissioner before the Tribunal and in any judicial proceedings in the courts that relate to proceedings before the Tribunal.

8.25 SECTION 87 - Proof of exceptions

8.25.1 Section 87 provides that the onus of proving an action is excepted from conduct that is an interference with the privacy of an individual rests on the defendant. Section 85 provides that the standard of proof is on the balance of probabilities.

8.25.2 I have suggested in recommendation 67 that section 37 should be amended to make it clear that in cases where a request for urgency has been substantiated, an agency is obliged to make reasonable endeavours to process the request with priority. It may be appropriate to place an onus on agencies on review to show that information which was supplied after delay was indeed provided “as soon as reasonably practicable”.

“Allowing complainants to go direct to the Tribunal at the outset may lead to complaints being brought before the Tribunal which could have readily been resolved by the Commissioner. It is unlikely that the Tribunal could deal with complaints more speedily than the Commissioner’s Office and the benefits of the Commissioner’s relatively informal inquisitorial approach (as opposed to the adversarial approach necessarily adopted before the Tribunal) are lost.”

- TELECOM NEW ZEALAND,
SUBMISSION UV13

8.26 SECTION 88 - Damages

- 8.26.1 The Complaints Review Tribunal is empowered to award damages for an interference of the privacy of an individual in respect of:
- pecuniary loss;
 - loss of any benefit;
 - humiliation, loss of dignity and injury to feelings
- 8.26.2 The largest award of damages to date was \$20,000 awarded in *L v N*³⁸ for humiliation, loss of dignity and injury to feelings. The decision is being appealed.
- 8.26.3 Section 88(2) and (3) provides for the disposal of damages in cases where the proposed recipient is an unmarried minor or is not of full mental capacity. Essentially, damages may be paid to the Public Trustee who deals with it in accordance with section 12 of the Minors' Contracts Act 1969 or section 66 of the Public Trust Office Act 1957. The provisions were modelled upon a provision in the (now repealed) Human Rights Commission Act 1977.
- 8.26.4 There appears to be a good case to align the provision to section 88 of the Human Rights Act 1993 which is arguably more consistent with fully respecting the autonomy of the individual. For example, where the individual is an unmarried minor the damages may be paid, as an alternative to the Public Trustee, to any person or trustee corporation acting as the manager of any property of that person.³⁹ Where the relevant person's property has been managed under the Protection of Personal and Property Rights Act 1988 payment can be made to the property manager.⁴⁰
- 8.26.5 Section 88 should be aligned with section 88 of the Human Rights Act. As an alternative, sections 88(2) and (3) could be repealed and it be provided in section 88 or 89, that section 88(2) to (6) of the Human Rights Act 1993 is to apply, with such modifications as are necessary, in respect of proceedings under section 82 or 83 as if they were proceedings under section 38 of the Human Rights Act.

**RECOMMENDATION 113**

Section 88(2) and (3) should be more closely aligned with section 88(2) - (6) of the Human Rights Act 1993.

8.27 SECTION 89 - Certain provisions of Human Rights Act 1993 to apply

- 8.27.1 Section 89 applies the relevant provisions of the Human Rights Act to proceedings of the Complaints Review Tribunal taken under the Privacy Act. In particular, the Human Rights Act gives the Tribunal jurisdiction to award damages up to the same maximum that the District Court can award which is, at present, \$200,000.⁴¹ Under section 90 of the Human Rights Act, the Tribunal can refer a matter to the High Court for a monetary remedy that exceeds the \$200,000 limit.

38 (1997) 3 HRNZ 721.

39 Human Rights Act 1993, section 88(3).

40 Human Rights Act 1993, section 88(5).

41 District Courts Act 1947, sections 29 to 34.

Part IX

IX

Proceedings of Commissioner

291

“The hallmark of the evolved Office of the Ombudsmen in New Zealand is that the investigatory process is informal, inquisitorial, and private.”

- Eagles, Taggart, Liddell *Freedom of Information in New Zealand*, 1982

9.1 INTRODUCTION

9.1.1 Sections 90 to 96 relate to the procedure and powers of the Commissioner in investigations under Part VIII of the Act. Of particular importance are:

- section 91 which relates to the obtaining of information by the Commissioner; and
- sections 94 to 96 which provide for the protection and privileges of witnesses in proceedings before the Commissioner.

9.1.2 The provisions have largely proved satisfactory and I make few recommendations for change. A number of the provisions are derived from similar legislation under which the Ombudsmen and Human Rights Commission operate and therefore have been tested in practice over many years.¹ Certain provisions in the Official Information Act and Ombudsmen Act have recently been reviewed by the Law Commission and I have paid particular regard to the recommendations arising from that review.

9.1.3 For the record, I do not have a power to enter premises. The Privacy of Information Bill proposed to confer powers of entry for the purposes of obtaining information relevant to a Commissioner’s investigation. However, I recommended that the select committee drop that power. I did not consider it necessary at the time and my experience since 1993 would seem to bear that out. I have not recommended that any such provision be made at this time.

9.1.4 It has been difficult for some agencies, including those represented by lawyers, to understand that the procedure is not based on the adversarial litigation model. To the contrary it is an investigative approach to establish the truth rather than merely to hear a dispute conducted before it by the parties. This has advantages that are not always initially understood.

9.1.5 Thus I tend to get submissions requiring me to comply with the rules of natural justice in the course of the investigation and attempts to discourage or prevent me from talking directly to staff of agencies except in the presence of the employer’s representatives. Usually after explanation, and an understanding that my investigating officers are not acting for the complainant, I have not

¹ See Appendix H which sets out a table of comparable provisions.

been frustrated in the investigation. Compliments are commonly paid about the objectivity and empathy displayed by my officers in carrying out investigations, even if there is (naturally enough) dissatisfaction with the outcome by one party or the other.

SECTION BY SECTION DISCUSSION

9.2 SECTION 90 - Procedure

9.2.1 Section 90 provides that my investigations of complaints are to be conducted in private. I need not hold any hearing and do not do so. No person is entitled as of right to be heard other than the person to whom the investigation relates. The only exception is that the person to whom the investigation relates has the right to submit a written response. I should also mention here that my procedures for provisional opinions, and the requirements of section 120 to allow a party to be heard before making any adverse comment, provide a fair procedure for all affected. Subject to compliance with any other provisions of the Act, I am free to regulate my procedure, obtain information and make such enquiries as I think fit.

9.2.2 The provision is satisfactory and does not, in my opinion, require amendment. It is derived from section 18 of the Ombudsmen Act 1975 and, like the procedures pioneered by the Ombudsman, allows sufficient flexibility that most investigations can be carried out in an inquisitorial, rather than adversarial mode. Most are completed by correspondence and on the telephone without the need to interview anyone in person.

9.3 SECTION 91 - Evidence

9.3.1 Section 91 is derived from section 73 of the Human Rights Commission Act 1977 and is comparable to section 19 of the Ombudsmen Act. The section makes a provision for the summons and examination by the Commissioner of persons on oath who are able to provide information relevant to an investigation. Examination under oath is deemed to be a judicial proceeding for the purposes of the law relating to perjury. I may also require people to furnish information and documents relevant to an investigation of a complaint.

9.3.2 It has not been common in my investigations to summon people to give evidence on oath. Since 1993 I have probably required it on only 2 to 3 occasions a year. It is not a step I take lightly because, amongst other things, it puts the person concerned to some inconvenience (although they are entitled to the fees, allowances, and expenses as would be applicable if the person was a witness in court). I have also required the production of information or documents pursuant to section 91(4) on about 2-3 occasions each year.

9.3.3 I have required evidence to be given on oath or documents to be produced in a variety of circumstances. Typically, but not exclusively, I have used the power where:

- information given in correspondence or on the telephone gives reason to question the veracity of the person;
- the matter at issue significantly turns upon the credibility of a particular person and this is, in the circumstances, best judged by interviewing the witness personally on oath;
- a respondent, or witness, is completely unco-operative and must be summoned for interview in order to get any response at all;
- a witness may have some evidence for which privilege is claimed and the circumstances of the obtaining of the evidence need to be established for the purposes of the privilege ruling;

- a respondent, for ethical reasons, will not release information except where formally required;
- one witness's account needs to be measured against another's view.

9.3.4 The provision works satisfactorily and is not in need of amendment.

9.4 SECTION 92 - Compliance with requirements of Commissioner

9.4.1 Section 92 provides that, pursuant to section 91, where the Commissioner requires an agency to furnish any information relevant to an investigation of a complaint, the agency is to comply with the requirement “as soon as reasonably practicable” and, subject to section 93, in no case later than 20 working days after the day the requirement is received. If an agency that is a department, Minister, or organisation fails to comply with the time limit for furnishing information I may report such a failure to the Prime Minister.

9.4.2 There might be scope for improving the provision with a view to enhancing the speediness of complaints resolution. However, there is a need to avoid undermining the rights of agencies or imposing undue compliance costs. One risk of the existing provision is that it can be used by recalcitrant agencies to spin out a response for a minimum of 20 working days but in many cases for far longer than that. A recalcitrant agency may, for example, fail to deliver documents “as soon as reasonably practicable” and instead await the full 20 working days. Following the expiry of this period, such agencies may count on getting away with a further delay notwithstanding that they may fall short of the requirements of the law. No automatic penalty is visited upon an agency by failure to meet such a time limit (although adverse comment or a report to the Prime Minister exists as a possible, if remote, sanction). Having received documents during or after the prescribed period, it is quite possible that my office may need to seek additional documents from an agency if a response has been incomplete or the request to the agency has not been framed broadly enough. Another 20 working days may have to be allowed.

9.4.3 Although urgency may suggest more rapid action in some cases, the general balance of convenience should permit a reasonable period for compliance with a requirement. However, it should be remembered that such requests do not come “out of the blue”. In access reviews they follow on from requests that have already been made by the individual concerned. In all complaints and investigations the agency will, almost certainly, have received notification of the fact of my complaint before any demand to furnish or produce information or documents. Sometimes the period between notification of the complaint and such a requirement may be a matter of weeks. Presently, where there is a long complaints queue, an earlier general “queue letter” may have been provided many months before any requirement is made.

9.4.4 The Law Commission recently completed a study of the comparable issue under the Official Information Act. In 1987 section 29A of the Official Information Act was added requiring responses to Ombudsmen's requirements as soon as reasonably practicable, and in no case later than 20 working days, because the Chief Ombudsman had observed that a major impediment to the success of the official information review process had been its slowness and it needed to be made clear that agencies were to respond promptly to requirements of the Ombudsmen.² The Law Commission recorded the Ombudsmen's expressions of concern about the time taken by departments to respond to their requirements. However, it noted that the emphasis should not solely be on the 20 working day limit since the prime obligation is to respond “as soon as reason-

² Law Commission, *Review of the Official Information Act 1982, 1997*, paragraphs 333-334.

ably practicable”.³ The Law Commission did not recommend any change to the relevant provisions of section 29A.

9.4.5 It would be desirable for the Commissioner to be able to require an agency to comply with a requirement within a period shorter than 20 working days in case of urgency. I have particularly in mind access reviews where the information or documentation at issue is reasonably finite and the urgency of the situation, or the interests of justice, require a prompt response. Sometimes there may only be a single letter which is sought for my investigation and 20 working days seems an absurdly long period to await its production.

9.4.6 The need for provision for urgency in some such cases was accepted when the Complaints Review Tribunal Regulations 1996 were issued. Although the regulations generally provide for a 30-day period for the filing and service of a statement of reply, it is provided that:

“The Chairperson may, on the application of the applicant in proceedings involving an alleged breach of information privacy principle 6 of the Privacy Act 1993, abridge the time for filing of a statement of reply in those proceedings if the Chairperson is satisfied that the urgency of the case so requires.”⁴



RECOMMENDATION 114

Section 92 should be amended so that the Commissioner may require an agency to comply with a requirement made pursuant to section 91 within a shorter period than 20 working days where the urgency of the case so requires.

Sanction for breach of time limits

9.4.7 Section 92 does not contain within it an enforceable mechanism for ensuring compliance with the requirements of the Commissioner. Instead, subsection (3) provides that the Commissioner may report the failure to comply with the Commissioner’s requirements to the Prime Minister if a Minister or central government agency⁵ fails to comply. No mechanism is provided for failure to comply with a requirement by any other public sector agency or by an agency which is not a public sector agency.

9.4.8 The provision is not satisfactory since the sanction is applicable to only a small class of the agencies subject to my jurisdiction. So far there has been no need to issue a formal section 91 requirement against a Minister or central government agency. Where there is significant non-compliance with a requirement I would be likely to refer the matter to the Police for prosecution under section 127 which provides a \$2000 fine for any person who:

“without reasonable excuse, refuses or fails to comply with any lawful requirement of the Commissioner or any other person under this Act.”

9.4.9 Occasionally, it may also be appropriate to report the individual to a relevant authority such as a professional association or trade body. If the issue were ever to arise in relation to a Minister or central government agency I might well provide a report to the Prime Minister but believe that I have the power to do so pursuant to my general functions in section 13(1)(r) in any case. Section 92(3) is, I believe, an inappropriate “cut and paste” borrowing from the Official Information Act into this new jurisdiction. The provision should be re-

³ *Ibid*, paragraph 339

⁴ Complaints Review Tribunal Regulations 1996, clause 7(2).

⁵ That is, a “Department or a Minister or an organisation”.

pealed since a mixed message is given by providing a response relating to non-compliance in respect of only one class of agencies.



RECOMMENDATION 115

Section 92(3) should be repealed.

9.5 SECTION 93 - Extension of time limit

9.5.1 Section 93 provides for an agency to extend the 20 day limit specified in section 92 for compliance with a requirement made by the Privacy Commissioner for information relating to a complaint. The agency may extend the time limit “for a reasonable period of time having regard to the circumstances” if:

- the requirement relates to, or necessitates a search through a large quantity of information or a large number of documents or papers or things and meeting the original time limit would unreasonably interfere with the agency’s operation;
- necessary consultations are such that the requirement cannot reasonably be complied with within the original time limit; or
- the complexity of the issues raised by the requirement are such that the requirement cannot reasonably be complied with within the original time limit.

9.5.2 The first and second reasons for extension run parallel to the reasons for the extension of time in responding to the initial request under section 41. I have recommended the third reason should also be available at that stage.⁶

No provision for multiple extensions

9.5.3 Dr Paul Roth has opined that section 93 is probably to be interpreted in a manner analogous to section 41 of the Act.⁷ Dr Roth also notes that in relation to the parallel provision in the Official Information Act the Ombudsman has pointed out that the legislation does not contemplate multiple extensions. I have therefore considered whether it would be desirable to amend section 93 - or indeed section 41 - to provide for multiple extensions. I have decided not to make such a recommendation since the extension provision is based upon agencies setting a realistic time-frame in any extension, having regard to the circumstances. The Law Commission considered the parallel provisions in the Official Information Act in its recent review and did not recommend any amendment.

9.6 SECTION 94 - Protection and privileges of witnesses etc.

9.6.1 Section 94 provides that, with the exception of a claim of public interest immunity under section 119, the same privileges as would apply in legal proceedings apply in relation to the giving of information to the Privacy Commissioner. Moreover, a person will enjoy immunity from prosecution if, in supplying information to the Commissioner pursuant to section 91, such compliance constitutes an offence under any enactment. However, if the giving of information constitutes an offence against section 127 of the Privacy Act (for instance, because the information is false or misleading), then the immunity does not apply.

1997 amendments - subsections (1A) and (1B)

9.6.2 Subsections (1A) and (1B) were inserted by section 2 of the Privacy Amendment Act 1997 with effect from 17 September 1997. These provisions had a much earlier genesis and were introduced by a Supplementary Order Paper to the Social Welfare Reform Bill upon which I reported in 1995.⁸ That Supple-

⁶ See recommendation 71.

⁷ *Privacy Law and Practice*, paragraph 1093.3

⁸ Report by the Privacy Commissioner to the Minister of Justice on Supplementary Order Paper No 84 to the Social Welfare Reform Bill, May 1995.

mentary Order Paper had arisen out of earlier work, and a recommendation, by the Social Services Select Committee on an inquiry into the privilege provisions of section 11 of the Social Security Act 1964. The Committee had recommended that:

“The Privacy Act 1993 should be amended to remove any doubt about the Privacy Commissioner’s right to examine documents for which privilege is claimed in order to form an opinion on such claims when such documents are the subject of a matter of complaint under Part VIII of the Privacy Act 1993.”⁹

9.6.3 I supported the Committee’s recommendation which was implemented through the new subsection. In my report to the Minister, I made recommendations to improve the provisions as introduced and a number of the changes were accepted.

9.6.4 The Law Commission, in its review of the Official Information Act, studied section 19(5) of the Ombudsmen Act which is the parallel provision to section 94.¹⁰ I will not repeat that material here although much of it is applicable also to section 94. However, I will quote the material which bears directly upon the 1997 amendments:

“The Law Commission therefore supports, in general, the insertion of section 19(5A) plus section 2 of the Ombudsmen Amendment Act 1997, which came into force the day before this report went to press. Section 19(5A) allows an Ombudsman - in the course of an investigation - to require the supply of, and to consider, information in respect of which privilege is claimed, in order to assess the validity of the claim. The Ombudsmen may not use that information in any way that is not permitted by subsection (5A); a new section 19(5B) specifies limits of the Ombudsmen’s disclosure of the information. Similarly, section 94 (1A) of the Privacy Act, inserted by section 2 of the Privacy Amendment Act 1997, allows the Privacy Commissioner to require the supply of, and to consider, information in respect of which privilege is claimed, in order to assess the validity of the claim.”¹¹

9.6.5 The Law Commission went on to recommend that section 19(5A) of the Ombudsmen Act and section 94(1A) of the Privacy Act should be narrowed. I could not see any basis for that and my office sought clarification of the Commission’s reasoning. On further consideration the Law Commission took the view that section 94(1A) and the equivalent to the Ombudsmen Act do not require amendment and resiled from that part of its recommendation.¹²

9.6.6 The 1997 amendments were necessary to stop a practice which threatened to undermine the efficacy of the complaints review process. Certain lawyers were advising their clients that documents withheld on an access request need not be given to the Commissioner for review if the agency had claimed legal professional privilege in relation to those documents. This approach flew in the face of ten years’ experience with the Official Information Act, would have under-

⁹ NZ House of Representatives, *Inquiry into the Privilege Provisions of section 11 of the Social Security Act 1964*, Report of the Social Services Committee, 1994 page 13.

¹⁰ Law Commission, *Review of the Official Information Act 1982*, 1997, paragraphs 321-327.

¹¹ *Ibid*, paragraph 326

¹² Letter Law Commission to Office of the Privacy Commissioner, 10 November 1997.

“Legal professional privilege has always been accorded the highest respect in our system of justice. In contrast, the recent amendment denigrates and diminishes the principle by giving the power to inspect confidential and sensitive material to employees of the Commissioner or the Commissioner him or herself, who are unlikely to possess the same level of competence as the judiciary in such matters, and do not have the same legal duties as officers of the Court.”

- ELLIS GOULD,
SUBMISSION UV17

mined the low cost and straightforward “Ombudsmen-type” review by an independent commissioner, and would have required court proceedings on each case to resolve. Such an approach may have suited some lawyers but was quite at variance with the approach of the legislation. The fact is that in most such cases under review where legal professional privilege is claimed the matter is quickly and routinely resolved at low cost by simply letting the Commissioner see the document. The Commissioner then expresses an opinion that the information is, or is not, properly withheld. It is hard to see this is a reasonable invasion into the lawyer client relationship. The opinion is not binding but is usually accepted by the parties. If it is not the matter can go to the Tribunal.

9.7 SECTION 95 - Disclosures of information etc.

- 9.7.1 Section 95 provides that a person bound by any enactment not to disclose particular information may be required to supply that information to the Commissioner, in which case the disclosure would not constitute a breach of the relevant enactment. Neither the Commissioner nor an employee can require the information where the Prime Minister certifies the disclosure might prejudice certain security, defence, or international relations, interests or where the Attorney-General certifies that the disclosure might prejudice law enforcement interests or injure the public interest through the disclosure of confidential cabinet matters. No certificate has yet been presented to me.
- 9.7.2 I have recommended elsewhere that the marginal note to this provision ought to be more informative, perhaps reading “Disclosures of secret information, etc.”¹³
- 9.7.3 The Law Commission in its review of the Official Information Act considered the equivalent provision in the Ombudsmen Act, section 20(1).¹⁴ The Law Commission notes that the wording of section 20 of the Ombudsmen Act dates from the original ombudsman legislation of 1962. That legislation was enacted only a few weeks after the Court of Appeal had first pronounced that the courts could review a Ministerial claim to withhold evidence on public interest grounds,¹⁵ and many years before a court was to review the decisions of Cabinet.¹⁶ Administrative law has come a long way in New Zealand since that time. The Law Commission also notes that the Official Information Act, passed twenty years after the original ombudsman legislation, does not give special protection to Cabinet or to Cabinet papers. Moreover, under the Official Information Act it is for an independent officer outside government - the Ombudsman - to judge prejudice to the protected interests, at least in the first instance. The courts now also undertake a similar function. Notwithstanding all of these considerations the Law Commission did not, on balance, favour repeal of section 20(1). In the light of such recent Law Commission consideration I do not recommend repeal of section 95(3) either.
- 9.7.4 However, the Law Commission went on to say that in the event of the use of the provision, it should be clear where responsibility (and political accountability) lies for the decision to prevent access to information. The Law Commission recommended that section 20(1) should be amended to specify that only the Attorney-General personally may exercise the power to prevent disclosure of information to the Ombudsmen.¹⁷ As the issues are the same under section 95 I have adopted a similar recommendation which should enhance the provision and ensure consistency if the Law Commission recommendation is adopted.

¹³ See recommendation 2.

¹⁴ Law Commission, *Review of the Official Information Act 1982*, 1997, paragraphs 316-320.

¹⁵ *Corbett v Social Security Commission* [1962] NZLR 878

¹⁶ *CREEDNZ Inc v Governor-General* [1981] 1 NZLR 172 (CA). See also footnote 176 to the Law Commission Report.

¹⁷ Law Commission, *Review of the Official Information Act 1982*, 1997, paragraphs 319-320.

“One of the reasons for the success of the Office since 1962 is that the Ombudsman has full access to the departmental file: thereby examining documents to which the aggrieved citizen has no legal rights of access.”

- EAGLES, TAGGART, LIDDELL

FREEDOM OF INFORMATION IN NEW ZEALAND, 1982

**RECOMMENDATION 116****Section 95(3) should be amended to specify that:**

- (a) the Prime Minister, in respect of paragraph (a); and**
- (b) the Attorney-General, in respect of paragraph (b);**

personally may exercise the power to prevent disclosure of information to the Privacy Commissioner.**9.8 SECTION 96 - Proceedings privileged**

- 9.8.1 Section 96 provides that the Commissioner, and any person engaged or employed in connection with the Commissioner’s work, enjoys immunity from civil and criminal proceedings for anything said or done in the course of their duties under the Act unless they acted in bad faith. Neither are they required to give evidence in any proceedings in respect of anything they learn in the exercise of their functions. Information supplied by any person in the course of proceedings before the Commissioner is to be privileged in the same way as if the information were supplied in court proceedings. “Qualified privilege” under the Defamation Act 1982 attaches to any report by the Privacy Commissioner.
- 9.8.2 I have considered the interrelationship between subsections (1) and (4) of the section as it appeared to me that a problem might potentially arise. Section 96(1) states that the section applies to:
- (a) the Commissioner; and
 - (b) every person engaged or employed in connection with the work of the Commissioner.
- However, subsection (4) appears to have more relevance to persons outside the office who deal with the Commissioner rather than the Commissioner or his staff themselves. Although section 96 is largely modelled on section 26 of the Ombudsmen Act 1975, that section has no equivalent to section 96(1).
- 9.8.3 I sought advice on the issue and was assured that while the interaction between the two subsections may be a little inelegant, there was no particular problem associated with section 96(4). It was suggested that subsection (4) “applies to” the Commissioner in the sense that it applies to an inquiry or proceedings before the Commissioner, and the status of certain evidence received in connection with that. Section 94(2) confers privilege on the production of documents and things. When and if they are produced section 96(4) operates to protect them subsequently. Accordingly, I do not recommend change.

Part X

X

Information Matching

299

“The central element in any redistribution system is the identification of who should provide resources and who should receive assistance. Our present processes, involving repetition and poor coordination between agencies, are a result of the historical development of different aspects of redistribution at different times. In addition, they are related to the technological possibilities at the time when each part of the redistribution system was developed. We now have the opportunity to consider redistribution as an overall system and to contemplate addressing equity and efficiency issues as well as privacy concerns. It would be worrying to abandon individual privacy issues in the battle to avoid any benefit fraud. It would also be irresponsible to continue to preserve the existing system in the name of defending privacy. It would be possible to continue to provide the same degree of privacy protection as is enjoyed at the moment with a considerably increased degree of accuracy in the overall assessment processes.”

- Mark Prebble, *Information, Privacy and the Welfare State*, 1990

“Persons familiar with both matching programmes and the Privacy Act argue that they want to allow the use of new technology and at the same time protect individual rights. The question is how to achieve such laudable balance. There is probably little disagreement that computer matching should be carried out in a manner as to pose as little challenge as possible to the privacy interests of citizens, but the issue remains of how best to do this. If one agrees that the indiscriminate use of matching is in no-one’s best interests, who is going to set the appropriate limits?”

- David Flaherty, *Protecting Privacy in Surveillance Societies*, 1989

“Computer matching is a powerful dataveillance technique, capable of offering benefits in terms of the efficiency and effectiveness of Government business greater than its financial costs. However, it is also highly error-prone and privacy-invasive. Unless a suitable balance is found, and controls imposed which are perceived by the public to be appropriate and fair, its use will result in inappropriate decisions and harm to people’s lives. In a tightly controlled society, this is inequitable. In a looser, more democratic society, it risks a backlash by the public against the organisations which perform it, and perhaps also the technology which supports it.”

- Roger Clarke, *A Normative Regulatory Framework for Computer Matching*, 1995

10.1 INTRODUCTION

- 10.1.1 In preparation for this review I circulated, in February 1997, a questionnaire on Part X to government agencies which participate in information matching. The questionnaire was not intended to seek any “official departmental view” but instead to reflect the opinions or experiences of individual officials and to identify issues and possible options for reform. The respondents may not have expected to have their comments released in identifiable form and therefore I have not quoted directly from the responses or attributed them to particular individuals or departments.
- 10.1.2 In September 1997, a discussion paper was released. As the subject matter is relatively specialised it is perhaps unsurprising that only 14 submissions were received. It has become apparent to me that the information matching rules might benefit from a more thorough review than has been possible in this process. For that reason, some of my recommendations are expressed as matters for further consideration. That would provide a further opportunity for consultation with agencies involved in information matching on proposals for changes to the rules with the resulting changes implemented by Order in Council issued under section 107.
- 10.1.3 It is fair to say that Part X is relatively technical. It not infrequently gives rise to difficulties of interpretation even by those who work quite closely with it. Accordingly, a number of my recommendations are directed towards making the Part more plain, understandable and transparent. Among the suggestions that I have to achieve this is cutting the Part’s scope back to more realistically reflect the areas of concern. For example, I recommend that the Part no longer apply to any process of manual comparison and be restyled “data matching”. I also suggest that the specified agencies be listed alongside the relevant provision in the Third Schedule.
- 10.1.4 Before addressing the detail of Part X it is worth canvassing the reasons why the Act has a special part of it directed towards “information matching” or, more correctly, “authorised information matching programmes”. To understand this one needs to consider:
- what is information matching? and
 - why is it of concern?

What is information matching?

- 10.1.5 What the Act terms “information matching” is more usually known as “data matching” or “computer matching”.¹ There is no single settled meaning for the term “data matching” but the following definitions have been suggested from overseas:
- *data matching* is the computerised comparison of two or more sets of records; the objective is to seek out any records which relate to the same individual. Where there is such a “match” then the information from one set of records may be transferred to enhance the other set. Alternatively, the information on the matched individual may be extracted for decision and action and may form the basis of a further set of records. This new set may ultimately form a set of “profiles” of individuals drawn from a number of different sources;²
 - *computer matching* is the comparison of machine-readable records containing personal data relating to many people, in order to detect cases of interest;³

¹ Data matching is the term used in Canada, Australia and Hong Kong. The USA uses “computer matching”. New Zealand is the only jurisdiction to call the process “information matching”. Even in NZ the process is frequently referred to as “data matching” - with the main unit undertaking matching styled as the “National Data Matching Centre” of the NZ Income Support Service.

² Data Protection Registrar, *Eighth Report of the Data Protection Registrar*, June 1992, page 49.

- *data matching*: the large scale comparison of records or files of personal information, collected or held for different purposes, with a view to identifying matters of interest.⁴

These various formulations convey what the technical process is about.

- 10.1.6 Not all data matching programmes are alike. New Zealand, to date, has primarily authorised information matching programmes in two circumstances:
- to detect fraud and overpayments, particularly in the social security area;
 - to recover monies owed to the Crown by locating the whereabouts of debtors.
- 10.1.7 Although the two types just mentioned cover nearly all of the matches currently operated, there have been some other forays into data matching. For example, the process has been utilised in relation to verification of continuing eligibility for benefit programmes. One match, concerning eligibility for the Community Services Card is directed towards identifying persons who may not have claimed a benefit to which they are entitled. However, New Zealand has not utilised data matching in all its varieties as yet. Dr Clarke, a noted commentator on computer matching, has identified eight primary purposes for most matching of which New Zealand offers examples of only three or four. The eight primary purposes are:
- **detection of errors** in programme administration;
 - **confirmation of continuing eligibility** for a benefit programme, or compliance with a requirement for a programme;
 - **detection of illegal behaviour** by taxpayers, benefit recipients, Government employees, etc;
 - **monitoring of grants** and contract award processes;
 - **location of persons** with a debt to a Government agency;
 - **identification of those eligible** for a benefit but not currently claiming;
 - **data quality audit**;
 - **updating of data** in one set of records based on data in another set.⁵
- 10.1.8 The practice of large scale data matching has only become possible with certain advances in computer technology and capacity. The first computer matching programme is sometimes claimed to be the one conducted in 1977 by the US Department of Health, Education and Welfare. That match compared the records of recipients of aid to families with dependant children with the payroll records of three million Federal employees.⁶ By 1982 it was estimated that US State and Federal agencies routinely carried out about 200 programmes which had apparently jumped to at least 500 by 1986. Experience suggests that the benefits of early matching, and its supposed successes, were wildly exaggerated whereas the problems at an operational level and for individuals affected were greater than had been anticipated.

Pros and cons of data matching

- 10.1.9 A great deal could be written about the perceived benefits and drawbacks of data matching. A number of people have attempted to do this. One report has

³ Roger Clarke, “A Normative Regulatory Framework for Computer Matching”, 13/4 *The John Marshall Journal of Computer & Information Law*, 587.

⁴ Australian Privacy Commissioner, *The Use of Data-matching in Commonwealth Administration Guidelines*, February 1998, clause 14.

⁵ Roger Clarke, “Computer Matching by Government Agencies: A Normative Regulatory Framework” (working paper August 1992), exhibit one. Dr Clarke also identifies a variety of circumstances in which data matching may contribute to additional purposes. For example, those with financial effects would include cancelling of incorrect payments, reduction of excessive payments, avoidance of future erroneous or excessive payments and deterrence of future fraudulent behaviour. Other purposes mentioned would include the maintenance of databases for social control purposes, construction of databases for research and statistical purposes, and improvement of programme policy, procedures and controls.

“Computer matching is like investigators entering a home without any warrant or prior suspicion, taking away some or all of the contents, looking at them, keeping what is of interest and returning the rest, all without the knowledge of the occupier.”

- AUSTRALIAN PRIVACY
COMMISSIONER

drawn together a list of claims made for data matching and the criticisms:

“The claims for data matching

Discussions in other countries have led to a number of benefits being claimed for the use of data matching. They include:

- detection and deterrence of fraud and other irregularities, for example, fraudulent or multiple claims, unreported income or assets, impersonation;
- verification of information supplied;
- verification of eligibility, for example for a benefit programme;
- identification of corruption or mismanagement, for example, conflict of interest; unusual payments; excessive withdrawals;
- construction of comprehensive databases for research purposes;
- identification of suspects through searching on the basis of the characteristics of potential offenders;
- improved efficiency, for example, in identifying and concentrating on genuine beneficiaries; or locating and rectifying discrepancies and errors;
- cost-effectiveness.

The criticisms of data matching

As benefits have been claimed, so there have been balancing criticisms of data matching. They include:

- lack of a general government or public oversight;
- cost/benefits are not thoroughly analysed so as to properly justify data matching programmes;
- poor quality and inaccurate information leads to mismatches and replication of errors;
- information is used out of context and may be untimely, insufficient, or unsuitable for the purpose of the match;
- information flowing from matching should be properly verified;
- machines should not be used as substitutes in qualitative decision-making for human discretion and judgment;
- the assembling of new files of profiles of individuals leads to the replication of inaccuracies and the drawing of what may be unjustifiable conclusions;
- individuals lack knowledge and control over the information about themselves;
- data matching constitutes a ‘fishing expedition’ without any pre-existing evidence or suspicion of wrongdoing;
- a presumption of innocence is turned into a presumption of guilt;
- individuals are not given any adequate opportunity to contest the results of a ‘match’;

“It is a technique which, unbridled, would present an Orwellian threat which even Orwell would not have imagined. The invasive indiscriminate use of the computer in gathering, storing and comparing personal information for purposes either benign or malign, reduces individuals to commodities, subjugates human values to mere efficiency.”

- CANADIAN PRIVACY COMMISSIONER

⁶ Details of this match, and information on the nature and origins of computer matching, can be found in Roger Clarke “Computer Matching by Government Agencies: The Failure of Cost/Benefit Analysis as a Control Mechanism” 4/1 *Information Infrastructure and Policy* (1995) 32. Apparently this match identified 33,000 raw hits, later filtered to 7,100 resulting in 638 internally investigated cases, of which 55 resulted in prosecutions. Only 35 convictions, all for minor offences, were entered. Initially hailed as a success, the paltry measurable benefits only became apparent upon study and such origins have in part led to a subsequent focus on seeking to judge such costly schemes on a cost-benefit basis.

- profile searching in particular results in a mass or class investigation, conducted on a category of people rather than individual suspects;
- allowing different organisations to exchange personal data weakens the traditional concerns for confidentiality in each.⁷

Controls on data matching

10.1.10 The objectives of most regulatory controls on data matching are directed towards seeking to ensure or maximise the claimed benefits of data matching and to constrain or eliminate the perceived shortcomings. Most schemes have an authorisation process which judges the costs/benefits and permits only those programmes which appear likely to be worthwhile. The shortcomings of data matching are limited through various legal, operational and management controls together with independent supervision and redress for individuals who have been wrongly harmed by the process. Ongoing, or periodic, scrutiny is used to seek to ensure that the original claims were well-founded and the programme is operated in accordance with the rules laid down.

10.1.11 The United States was the first country to adopt a statutory scheme for the regulation of data matching. It was followed by Australia in 1990 and New Zealand in 1991. Meanwhile, the Canadians at Federal level had adopted an administrative scheme for the regulation of data matching and the Australians have since supplemented their statutory scheme with administrative controls for other programmes involving Federal agencies. In 1995 Hong Kong also regulated aspects of data matching by statute, although apparently in a less rigorous way than New Zealand, but with the novel feature that the controls apply equally to the public and private sectors.

Information matching not prohibited

10.1.12 Part X purports to regulate aspects of “information matching”. In fact, the Part does not regulate all information matching but only certain types of programmes, primarily those which will be used for the purpose of taking adverse action against individuals and which have been authorised by statute. As the scope of the Part is thereby quite limited I have recommended elsewhere it should be headed “*authorised information matching programmes*” rather than simply “information matching”.⁸ That small change may help to avoid misunderstanding by some people.

10.1.13 It is necessary to understand that Part X, and indeed the Privacy Act itself, does not contain a prohibition on data matching.⁹ This contrasts with the Hong Kong law which does prohibit data matching unless it has been appropriately authorised by the individual, the Commissioner specifically, or is of a class authorised by the Commissioner or by law.¹⁰ Generally the schemes in the USA, Canada and Australia only involve matches in which the Federal Government participates. Each scheme differs in the types of matches which are required to be brought within the controls or are exempted from them.

10.1.14 In 1991 the Privacy Commissioner Act first regulated information matching in New Zealand. Brought within its scope were all information matches known to be operated or intended soon to be operated. Government policy since that time has been to bring proposed new matches within the framework by enact-

⁷ Data Protection Registrar (UK), *Eighth Report of the Data Protection Registrar*, June 1992, pages 49-50.

⁸ See recommendation 2.

⁹ Section 108 does operate as a partial bar to information matching outside the controls of Part X where there already is an authorised information matching provision. Section 109 prevents the reliance upon the official information statutes to circumvent the controls on information matching in Part X.

¹⁰ Personal Data (Privacy) Ordinance 1995 (Hong Kong), section 30(1).

“What is wrong about ‘fishing expeditions’ is wrong about unrestrained computer matching: it changes the way a government looks at its citizens. Participating in a government programme is a status not a crime. To subject a whole class of citizens to search for possible violations is akin to a ‘general warrant’, a practice in England that permitted the Crown to search without specifically naming the target.”

- CANADIAN PRIVACY COMMISSIONER

ing an information matching provision which is added to the list in the Third Schedule. However, it is necessary to realise that only those matches which have been specifically authorised by a statutory “information matching provision” are covered by the controls in Part X. It is conceivable that matching programmes could exist or be created, not brought within Part X and yet still be in compliance with the law. For example, in addition to authorised information matching programmes covered by Part X, matches might exist as follows:

- a match authorised by a specific provision in legislation which has not been identified as an “authorised information matching provision”;¹¹
- a match carried out pursuant to general authority of an enactment which can be characterised as “authorising” or “requiring” the match which may override any inconsistent provision in an information privacy principle by virtue of section 7 of the Act;¹²
- a match undertaken by a department which is able to be carried out consistently with the information privacy principles or in reliance upon applicable exceptions to the principles (for example consistently with the purposes for which information is obtained or with individual authorisation);
- a match which is not in conformity with the principles but is otherwise authorised, for instance by an exemption granted by the Commissioner or pursuant to a code of practice.¹³

10.1.15 Generally speaking it would be difficult for a Government agency to carry out an information matching programme, and take adverse action against individuals, without seeking specific legislative authority. In the event that legislative authority is sought the Department will, by virtue of obligations in the *Cabinet Office Manual*, be obliged to address the question of compliance with the information matching controls. This in turn will normally require the relevant provision to be identified as an information matching provision in the Third Schedule.¹⁴

10.1.16 The principal compliance difficulties that departments would have in commencing a new information matching programme consistently with the information privacy principles include:

- the new programme will involve a collection of information from a source other than the individual concerned - therefore an applicable exception to information privacy principle 2 would need to be found;
- similarly, the programme will involve a disclosure of personal information for a new purpose and it may be difficult to find a relevant exception if authorisation of the individual is not possible or likely;
- at least one of the sets of information which is to be compared will be being disclosed to a new recipient, and being used for a new purpose, and it is unlikely that individuals will have been made aware of this in accordance with information privacy principle 3 - therefore a compliance issue arises as to the openness of the information handling practices of both departments if the match is to continue.

¹¹ There are several examples of these already. Through the process of consolidating various statutes some provisions which were listed in the 1991 Act had been inadvertently left out of the schedule to the 1993 Act for varying periods. Also, section 11A of the Social Security Act is not listed as an information matching provision but nonetheless provides that it is, for a number of purposes, to be treated as if it is.

¹² Pursuant to government policy these and those in the next category should be created as information matching provisions and subjected to Part X.

¹³ A series of one-off exemptions were granted by the Privacy Commissioner pursuant to section 54 for a series of comparisons of information similar to information matching in 1995/96. See report of the Privacy Commissioner for the year ended 30 June 1997, page 25.

¹⁴ See *Cabinet Office Manual*, August 1996, chapter 5, paragraph 5.26, 5.29 and 5.58 and Appendix 6 (Standard format for legislation submissions).

10.1.17 Notwithstanding the practice and policy of bringing new matches within the Third Schedule there have been cases where it has been inappropriate to do so. The most common such circumstance is where a match is to be undertaken for statistical or research purposes and not to enable adverse action to be taken against an identifiable individual. Where departments are contemplating seeking authority for a new matching programme I have encouraged them to undertake a pilot statistical match so as to generate empirical data by which the likely usefulness, and the cost benefit, of a prospective match may be projected and judged. Safeguards are taken by the departments to ensure that the data is destroyed or de-identified once the necessary statistics have been extracted. I have seen the “statistical and research purposes” exceptions to principles 2, 3 and 11 as providing sufficient authority for such pilot matches to be undertaken.

10.1.18 Another case involved the transformation of an existing process of manual verification of jury lists into an automated process. For many years information extracted from the electoral roll had been sent to court registrars from which a jury list is drawn. Preliminary steps are taken to omit names from the list of persons who are ineligible to serve. The practice has been for potential jurors’ names to be checked against the criminal history listing on the Wanganui Computer. This had been done by a Court official checking each name individually through the Court terminal to the computer. This would not have been characterised as an “information matching programme” as defined in section 97. However, to modernise court administration it was proposed to automate the process. The list of potential jurors would be matched against the Wanganui Computer list of relevant convictions. It is difficult (although not impossible) to characterise the omission of a name from the list of potential jurors as “adverse action” as it is normally understood. Having considered various aspects of the process it was not considered appropriate to bring it within Part X.

10.1.19 One confusing aspect of Part X is therefore the position of the matching programmes which are *not* authorised. This will continue to be a source of confusion for those unfamiliar with Part X. It is difficult to address the matter without fundamentally changing the approach of Part X which I have not attempted in this review.

Legitimising data matching

10.1.20 It is as well to reflect at this point that the Privacy Act 1993 fulfils a function of *legitimising* information matching. Whether this is predominantly good or predominantly bad for privacy is a moot point. In my view, it *is* an appropriate function of data protection legislation to legitimise data matching if it avoids the ad hoc and uncontrolled application of the technique and brings the activity within a satisfactory structure which places a set of controls, subject to independent oversight, directed to:

- *authorisation* - ensuring that only matches which appear to be well justified in the public interest go ahead;
- *operation* - ensuring that matches are operated consistently with fair information practices and, given the nature of the technique, that individuals are not presumed guilty until they prove their innocence;
- *evaluation* - that matches are subject to periodic review and discontinued unless they show continuing benefits and the ability to be operated consistently with fair information practices.

It may also be that, on occasion, information matching may be less privacy invasive than alternative methods of detection of possible fraud.

“A traditional investigation is generally triggered by some evidence that a person is possibly engaged in wrongdoing. A computer match is not bound by this limitation. It is directed not at an individual, but at an entire category of persons. It is random in nature as it is not initiated because any person is suspected of misconduct, but because a category is of interest to the Government. What makes computer matching fundamentally different from a traditional investigation is therefore that its very purpose is to generate the evidence of wrongdoing required before an investigation can begin.”

- ONTARIO INFORMATION AND PRIVACY COMMISSIONER

SECTION BY SECTION DISCUSSION

10.2 SECTION 97 - Interpretation

Further definitions

10.2.1 Section 97 sets out definitions used throughout Part X. The general definitions in section 2 also apply. I am aware of occasions where staff in agencies undertaking information matching have forgotten to look to that earlier section for relevant definitions such as that of “working day”.

10.2.2 Only nine terms are given specific definitions for Part X. There has been a tendency amongst agencies working in this area to coin a variety of other terms to describe the various information matching concepts. Indeed, in a paper for the Second Privacy Issues Forum in Wellington in 1995, the National Data Match Co-ordinator for the Department of Social Welfare, offered working definitions for twelve terms neither used or defined in the Privacy Act:¹⁵

- challenge;
- invalid match;
- legitimate match;
- match-run;
- match-run date;
- matching agency;
- mismatch;
- no further action;
- partial positive match;
- positive match;
- record count;
- source agency.

10.2.3 I suggest below that “source agency” and “matching agency” should be defined.¹⁶ I also suggest that it might be possible to use the information matching rules to address definitional problems given the special amendment procedure in section 107.¹⁷ However, I see no need for any large number of further definitions.

Adverse action

10.2.4 The definition of “adverse action” has caused difficulty for staff in some agencies involved in information matching. The concept of adverse action is primarily applied in sections 101, concerning the use of the results of an information matching programme, and section 103, providing for notice of proposed adverse action to be sent to individuals.

10.2.5 The Privacy of Information Bill had no definition of “adverse action”. Instead the concept appeared in a composite provision being the equivalent to sections 100 and 101. That had as its origin sections 10 and 11 of the Data-matching Program (Assistance and Tax) Act 1990 (Commonwealth of Australia). The Australian Act is therefore the origin of the concept of “adverse action” although the term is not actually defined there. The Hong Kong privacy law has adopted the first part of the New Zealand definition but has additionally referred to “legitimate expectations” and omitted the specific examples in paragraphs (a) to (f) of the New Zealand definition.¹⁸

10.2.6 The reason that some people have had difficulty with the definition is that they

¹⁵ Dallas Elvy “Information Matching”, Privacy Issues Forum, 29 June 1995.

¹⁶ See recommendation 121.

¹⁷ See recommendation 137.

¹⁸ Personal Data (Privacy) Ordinance 1995 (Hong Kong), section 2, defines “adverse action” in relation to an individual to mean “any action that may adversely affect the individual’s rights, benefits, privileges, obligations or interests (including legitimate expectations).”

have failed to notice that it encompasses actions that *may* adversely affect the rights etc of specific individuals. That, of itself, seems to indicate that the concept encompasses actions taken or anticipated quite early in the processes following the carrying out of an information match. It is an action which has the potential to affect the rights of a specific individual and not simply the later action which does directly affect that individual. This is made plainer by the second part of the definition which makes it clear that such action includes “any decision” to do certain things in relation to the individual. Difficulties that have arisen with the interpretation of the term are not because the definition itself is particularly unclear but because departments have found it inconvenient to accept the provision’s plain words. The term is defined as it is in order that the controls in sections 100, 101 and 103 should be applied at a very early point in the process and not, as some departments would wish, after preliminary steps which may affect individuals’ interests have already been taken.

- 10.2.7 Responses to the questionnaire noted that paragraph (a) to (f) did not cover all of the commonly occurring circumstances of adverse action. From a definitional point of view, this need not matter particularly so long as the relevant action can be said to “adversely affect the rights, benefits, privileges, obligations, or interests of any specific individual” (that is, within the first part of the definition). However, from a practical and operational point of view it would be helpful for all of the common examples to be listed so as to make the position more plain. I have two suggestions.
- 10.2.8 The first suggestion is to include the phrase “to impose a penalty”. This is numerically, and financially, important in the context of the DSW programmes.
- 10.2.9 The second relates to the recovery of a penalty imposed by a department and of a fine. In this context the word “decision” may confuse the issue for some when the position is that someone has already been covered by a decision to recover money, but the department could not find the miscreant, and now as a result of address matching is able to take further steps to recover the fine. The concept of “adverse action” is intended to apply in such circumstances and I take the view that it does even as presently drafted. However, it may be helpful to agencies operating address matches used to trace and enforce Court ordered obligations for the second part of the decision to be made more explicit.



RECOMMENDATION 117

The definition of “adverse action” in section 97 should be supplemented by a paragraph relating to decisions to impose a penalty and to recover a penalty earlier imposed.

Authorised information matching information

- 10.2.10 This definition seems relatively plain and has not given particular difficulty in interpretation. Some of the information matching provisions are more particular than others in the authority they give for the disclosure of information. In my view, information matching provisions should precisely list the information which may be disclosed.

Authorised information matching programme

- 10.2.11 The definition of “authorised information matching programme” surprisingly does not simply constitute an “information matching programme” (as defined) which has been authorised. In fact, the definition repeats several elements of the definition of “information matching programme” (such as the comparison of information with the purpose of producing or verifying information) but omits other elements (such as the requirement that the information may be used for the purpose of taking adverse action against an identifiable individual).
- 10.2.12 It is not immediately apparent why the differences in definition have been

“We view data matching as a procedure which poses a number of data protection dangers and believe that safeguards are warranted where it exposes data subjects to adverse decisions. Not all data matching does so, but when it does controls are in our view desirable.”

- THE LAW REFORM COMMISSION OF HONG KONG, *REPORT ON THE REFORM OF THE LAW RELATING TO THE PROTECTION OF PERSONAL DATA*, 1994

adopted. Perhaps it was anticipated that authorised programmes might encompass a wide range of matching including that which did not have as its purpose the taking of an adverse action against identifiable individuals. If that was the intention, the approach has since been somewhat haphazard. The Community Services Card Match is the only authorised programme which is not used for taking an adverse action against individuals. Perhaps the reason for adopting the perplexing definition is found within section 108. That is the only provision which utilises within it both “authorised information matching programme” and “information matching programme”. There may be scope for simplifying the definition. If that is to be done, care would need to be taken to ensure that section 108, and any other affected provision, is not inadvertently changed in substance.

Discrepancy

10.2.13 The definition is derived from the definition of “discrepancy” in the Australian legislative scheme.¹⁹ I do not consider that it requires amendment.

Information matching programme

10.2.14 The definition of “information matching programme” has several elements. Features to note include:

- an information matching programme involves the comparison of any document that contains personal information about ten or more individuals with one or more similar documents;
- the comparison may be made manually or by means of any electronic or other device;
- the comparison must be for the purpose of producing or verifying information that may be used for the purpose of taking adverse action against an identifiable individual.

10.2.15 This definition potentially encompasses a far broader range of programmes than most overseas schemes or definitions.²⁰ No comparable scheme overseas provides for oversight of, or safeguards in relation to, manual matching. For example, the definition of “matching procedure” in the Hong Kong law is quite similar to our own definition of information matching programme but expressly excludes comparison by “manual means.”²¹

10.2.16 The concern to which the information matching controls are directed relate to what is commonly known as *computer* matching or *data* matching. Nonetheless, as a definitional matter it was decided, consistent with the rest of the Act, to avoid distinctions based upon:

- whether the processing of information is by automated or manual means; or
- whether the information is stored in electronic or other media.

10.2.17 The special data matching controls in New Zealand, USA, Australia, Canada, Hong Kong and other countries have arisen from concerns about automatic processing of information and, particularly, the use of computers for covert surveillance. Dr Roger Clarke, a commentator on data matching, describes the processes of concern as “dataveillance”. He distinguishes two types: personal dataveillance, in which an identified person is monitored, generally for a specific reason; and mass dataveillance, in which groups of people are monitored, generally to identify individuals of interest.²² The controls of the type found in our Act and similar legislation are directed towards mass dataveillance. It is

¹⁹ Now found in Data-matching Program (Assistance and Tax) Guidelines, clause 2.2.

²⁰ However, note that while “information matching programme” is a broad definition, Part X itself tends only to cover *authorised* information matching programmes.

²¹ Personal Data (Privacy) Ordinance 1995 (Hong Kong), section 2(1).

²² See Roger Clarke, “A Normative Regulatory Framework for Computer Matching” 13/4 *The John Marshall Journal of Computer and Information Law* (1995) 585.

hardly possible to imagine mass dataveillance without the use of automated processes of comparison. Even if mass dataveillance might be theoretically possible on a manual basis, it would be uneconomic.

- 10.2.18 A further concern (and another distinguishing manual from automated matching) is the involvement of human beings. One of the fears of data matching is that machines will be programmed in such a way that decisions affecting individuals are made without any real person considering the facts of an individual case. The EU Directive on Data Protection articulates such concerns in article 15 by providing special controls on automated individual decision-making.
- 10.2.19 The special controls in Part X, which operate as a specific regime within a more general statute, may be more effective and better understood where the key concepts correspond to the risks designed to be addressed and the reality on the ground. The present reality is that there are no “manual” matches authorised. I see little prospect of any being brought within Part X. It might be desirable to limit Part X to the area of prime concern and therefore to exclude manual comparison from its coverage.²³
- 10.2.20 Exclusion of manual matching from the scope of Part X could be achieved by providing an exception to the definition of “information matching programme” and “authorised information matching programme”. This is the approach taken in Hong Kong. Alternatively, the definition could be recast so that the notion of “computerised” or “automated” comparison is incorporated as an element. This is the approach taken in the USA.²⁴ The result appears to be the same either way.



RECOMMENDATION 118

Consideration should be given to amending the definitions of “authorised information matching programme” and “information matching programme” in section 97 so as to exclude manual comparison from their scope.

- 10.2.21 If manual matching is excluded, the process should be given an explicitly narrower title such as “computer matching” or “data matching” which suggests the involvement of automated processes. I favour data matching as this appears to be the term which has the widest currency internationally and is frequently used domestically. It is possible to label the process as “data matching” without needing to define, or use, the term “data” anywhere in the Part. The process can be styled as “data matching” while still referring to the comparison of “information” so as to remain consistent with the rest of the Act.



RECOMMENDATION 119

Consideration should be given to replacing references in Part X and elsewhere to “information matching” by “data matching”.

Information matching provision

- 10.2.22 I am unaware of this definition causing any difficulties in interpretation.
- 10.2.23 There were ten sections listed as information matching provisions when the Privacy Commissioner Act 1991 was first enacted.²⁵ Most of the Schedule from the 1991 Act was carried over into the Act and subsequently three of the original provisions, never used, were omitted with the enactment of the Births, Deaths and Marriages Registration Act 1995. With the addition of new infor-

²³ I use the shorthand expression “manual matching” but it is the process of *comparison* where the computer comes into its own. A programme might well have other manual components in the obtaining, disclosure or the use of information. For this reason the spelling of “programme” should remain rather than the computer-oriented “program”.

²⁴ Privacy Act 1974 (USA), 5 USC §552a (8).

²⁵ Privacy Commissioner Act 1991, Third Schedule.

mation matching provisions there are now thirteen sections listed in the Third Schedule as information matching provisions. Bills before Parliament are poised to add several more.

Information matching rules

- 10.2.24 The phrase “information matching rules” is defined to mean the rules for the time being set out in the Fourth Schedule to the Act. Proposals for amending the rules are made with the material discussing sections 107 and the Fourth Schedule.²⁶

Monetary payment

- 10.2.25 I am not aware of this definition giving rise to any interpretational difficulties. Indeed, it has been suggested to me that the definition is quite unnecessary.

Specified Agency

- 10.2.26 “Specified agency” is defined simply to mean any of the agencies listed in the provision. The list has been amended from time to time with the addition of certain agencies, substitution of new names for restructured departments, and in one case the removal of an agency as the result of the repeal of particular information matching provisions.

- 10.2.27 The present definition of “specified agency” gives the somewhat misleading impression that Part X legitimises an arrangement whereby a group of eight agencies may share personal information amongst themselves. Indeed, this is precisely what an Opposition member of Parliament alleged on the Third Reading of the Privacy Commissioner Bill in which he stated:

“So the bill establishes what really amounts to a club - I mean in the insurance club sense of the word. A group of agencies - eight in number - now has a mandate to match information and to share it.”²⁷

- 10.2.28 In fact, there is not a multiple sharing arrangement amongst all eight agencies but rather a series of bilateral arrangements between particular specified agencies pursuant to particular information matching provisions. This is not particularly plain from reading Part X or the Third Schedule but becomes clearer once a study is made of the various information matching provisions. In fact, it is only possible to know whether a specified agency participates in one or more information matching programmes and, if so, which and in what capacity, by studying a raft of provisions in other statutes. Transparency would be enhanced by redefining “specified agency” in the following manner:

Specified agency means any agency listed in the third column of the Third Schedule as a specified agency in respect of an information matching programme authorised pursuant to an information matching provision specified in the first column of that Schedule.

- 10.2.29 One will then be able to see by a simple check of the Third Schedule:
- which programmes an agency is involved in; and
 - which agencies are involved in a particular programme.



RECOMMENDATION 120

The definition of “specified agency” in section 97 should be amended so that the agencies are listed in the Third Schedule alongside the information matching provisions to which they relate.

²⁶ See paragraphs 10.12 and 13.5.

²⁷ Rt Hon. David Lange, speaking on the third reading of the Privacy Commissioner Bill, 10 December 1991.

- 10.2.30 All the agencies participating in an information matching programme are referred to as “specified agencies” regardless of the capacity in which they participate. This contrasts with the schemes in North America and Australia which label agencies by their function in a programme. By categorising the agencies it has been possible in those other schemes to separately identify some of the requirements of the regulatory scheme to apply to certain classes of agencies and not others.
- 10.2.31 Some schemes use a term to identify the totality of participants in a scheme. This corresponds with our present definition of “specified agency”. In the Australian statutory scheme this is simply referred to as an “agency”.²⁸ In a scheme devised by Dr Clarke the term used is “a participating organisation”.²⁹ The second categorisation used by most schemes is to identify the agency which discloses the records for the use in a matching programme. This is referred to as a “source agency” in the schemes in the USA and Australia (both under the statutory scheme and pursuant to the Privacy Commissioner’s guidelines) and as “matching source” in Canada. In each case, a definition is provided to the effect that a source agency is one which discloses information to a matching agency for use in a data matching programme. Typically the third category is “matching agency” which is the agency on whose computer facilities the matching is conducted. The scheme in the USA instead refers to a “recipient agency” being the agency which receives the information from the source agency for use in a matching programme.
- 10.2.32 Logically, there should be a further category of agency which is authorised to *use* the resultant “hits”. In New Zealand, this has always been either the source or the matching agency,³⁰ although it does not follow that this will always be the case. “User agency” seems an obvious choice and this is adopted in the Australian Privacy Commissioner’s guidelines.
- 10.2.33 Definitions of the new terms should be supplemented by identification of each agency as an authorised “source agency”, “matching agency” and/or a “user agency”. The Third Schedule should list, against the information matching provisions to which they relate, each of the specified agencies and the capacity in which they participate. Some agencies will participate in a match in more than one capacity, as a user agency and matching agency or as a user agency and source agency.
- 10.2.34 Defining these concepts, and identifying the agencies in their respective capacities in the schedule, will enable the statutory scheme to be more transparent. However, the full benefit will only be realised when the opportunity is taken to rewrite some of the material in Part X and the Fourth Schedule utilising the newly defined terms. That will enable some provisions to be set out in a clearer or more precise fashion. In others it may be possible to allocate certain statutory obligations to some classes of agencies but not others. I recommend elsewhere that a more detailed review of the information matching rules be undertaken at a later date which I think will offer a good opportunity to bring the new terms into use in a clear and understandable manner. I expect that the terms will also be useful in information matching agreements entered into under section 99.

²⁸ Data-matching Program (Assistance and Tax) Act 1990, section 2(1).

²⁹ Roger Clarke, “A Normative Regulatory Framework for Computer Matching” 13/4 *The John Marshall Journal of Computer and Information Law*, 619.

³⁰ Indeed, locally a somewhat confusing terminology has grown up, at variance with the international approach, according to the agency which is to be the primary user of the information the title “matching agency” regardless of whether it has actually carried out the comparison of records.

**RECOMMENDATION 121**

Consideration should be given to:

- (a) including in section 97, in addition to the definition of “specified agency” (which could be renamed “participating agency”), definitions of “source agency”, “matching agency” and “user agency”; and
- (b) utilising these newly defined terms in Part X and the Fourth Schedule as appropriate.

10.3 SECTION 98 - Information matching guidelines

10.3.1 Section 98 sets out the six information matching guidelines. Section 13(1)(f) requires the Privacy Commissioner to have particular regard to the guidelines when examining proposed legislation which would provide for information matching. The Commissioner’s function under section 13(1)(f), and the process adopted for undertaking that examination, are outlined at paragraphs 3.3.36 - 3.3.42.

10.3.2 When introduced in the Privacy of Information Bill, the information matching guidelines were to have been the grounds upon which the Privacy Commissioner could grant, upon application by a department, approval for an information matching programme. This was changed by the select committee so that the decision as to whether an information matching programme proceeds is one for Parliament, not the Commissioner. However, the information matching guidelines have been retained to guide the Commissioner when examining a proposed programme and reporting to the Minister of Justice.

10.3.3 The information matching guidelines have not been taken directly from any precedent in a New Zealand or overseas law. However, the basic approach, and elements of the guidelines, can be found in similar sets of requirements for data matching proposals in other jurisdictions. For example, many of the elements are similar to those found in the Australian Privacy Commissioner’s *Guidelines for the Use of Data Matching in Commonwealth Administration*,³¹ the Canadian Treasury Board Manual,³² and the Computer Matching and Privacy Protection Act 1988 (USA).³³

10.3.4 The schemes providing for control of data matching in the USA, Canada, Australia and New Zealand each emphasise the need to evaluate any proposed programme on a cost-benefit basis before allowing them to proceed. The reasons for this approach have been outlined in a variety of governmental reports.³⁴ There has also been scholarly analysis of the reasons for undertaking cost-benefit analysis.³⁵ Briefly stated the reasoning goes something like this:

- data matching is an activity which can severely intrude on privacy;
- data matching has the potential to uncover fraud, and recover monies owed to the government, and therefore in some cases the effect on privacy may be outweighed;
- experience has shown that the claimed benefits of data matching have been wildly exaggerated while the costs, financial and otherwise, have been underestimated;
- therefore, cost-benefit analysis is needed to ensure that privacy is only al-

³¹ The current version is dated February 1998. See clause 32 (“Proceeding with a programme”).

³² Treasury Board of Canada, *Treasury Board Manual*, Chapter 2-5 (Data matching), Preliminary assessment, pages 1-2 (current version 1 December 1993).

³³ To be read together with guidelines issued by the Office of Management and Budget.

³⁴ See for example, United States General Accounting Office, *Computer Matching: Assessing its Costs and Benefits*, September 1986.

³⁵ See, for example, R Clarke “Computer Matching by Government Agencies: The Failure of Cost/Benefit Analysis as a Control Mechanism” 4/1 *Information Infrastructure and Policy* (1995) 29 and “A Normative Regulatory Framework for Computer Matching” 13/4 *The John Marshall Journal of Computer and Information Law* (1995) 585.

“After four full years of operation the cumulative savings from the programme are \$210 million across all agencies. It is interesting to note that to date the total net savings from all agencies remain less than the DSS anticipated it would save in one year.”

- KEVIN O’CONNOR, PRIVACY

COMMISSIONER OF AUSTRALIA,

EIGHTH ANNUAL REPORT ON THE

OPERATION OF THE PRIVACY ACT,

1996



lowed to be overridden in cases where it can confidently be shown that a data match will indeed bring quantifiable and commensurate public benefits.

- 10.3.5 The monetary savings are only one part of the equation. There is a privacy concern to ensure that the matches justified for their net financial benefit can be and are undertaken in accordance with fair information practices. Considerable experience has been gathered in the USA, Canada, Australia and now New Zealand, in evaluating and operating information matching programmes so that the worst excesses of data matching experienced in the past are not repeated. Accordingly, the initial assessment not only looks to net financial benefit but also to assurances that any programme will be operated in conformity with a set of information matching rules and controls.
- 10.3.6 Although there is not an absolute demarcation, generally speaking the first four of the six information matching guidelines are directed towards financial considerations with the last two guidelines addressing what might be termed “data protection” or “fair information practice” concerns.
- 10.3.7 It is unnecessary in this report to go into detail about the information matching guidelines since, with the exception of several relatively minor matters raised below, the guidelines have worked satisfactorily in operation and are not in need of amendment. I have offered detailed comment in relation to each of the guidelines in seven information matching programmes, or amendments to programmes, that I have examined and reported upon pursuant to section 13(1)(f). Copies of the reports and extracted comments on each of the guidelines have recently been published in a compilation.³⁶
- 10.3.8 I have four suggestions for change to the information matching guidelines. The first proposes a change to paragraph (c). The next two involve minor changes to paragraph (e) which will amplify upon the guideline but not change it substantively. The final suggestion is to alter paragraph (f) to expand its scope beyond compliance with the information matching rules to encompass compliance with Part X itself.

Paragraph (c)

- 10.3.9 Paragraph (c) requires consideration to be given to whether or not the use of an alternative means for achieving the match’s objective would give results of the type mentioned in paragraph (b), that is that it will achieve significant and quantifiable monetary savings or other comparable benefits to society. It would be worthwhile amending this paragraph so that consideration is also given to whether the alternative means of achieving the objectives are more, or less, privacy intrusive. The existing paragraph appears to assume that any other means of achieving the objective will give a better result for privacy. However, while that will often be true, it is not invariably the case.



RECOMMENDATION 122

Section 98(c) should be amended so that alternative means of achieving the objective of a proposed matching programme are examined with a view to considering whether they would be more, or less, privacy intrusive.

Paragraph (e)

- 10.3.10 Guideline (e) requires me to look at whether the scale of the matching programme is “excessive”. The guideline further requires me to have regard to the number of agencies that will be involved in the programme and the amount of detail that will be matched. I have not read guideline (e) as limiting me solely

³⁶ See Office of the Privacy Commissioner, Examination of Proposed Information Matching Programmes, March 1998.

to having regard to the number of agencies and the amount of detail matched if there is some other factor involved in the information matching programme which suggests that its scale is excessive.

- 10.3.11 It occurs to me that it would be relevant to consider, in seeking to gauge whether a match is “excessive”, the amount of information disclosed from one agency to another following a successful hit or match. I have had to consider this precise issue in the context of an amendment affecting the information matching programme between the Department for Courts and DSW³⁷ and in a similar proposal for a match between the Department for Courts and the Inland Revenue Department.³⁸ The amendment affecting the Courts/DSW match would, for the first time, have permitted DSW to disclose client telephone numbers to Courts. Prior to this amendment the information matching provision had merely authorised the disclosure of address details. The issue for me was whether the disclosure of additional information, in this case telephone numbers, might make the match “excessive”. In an examination of the subsequent Courts/IRD match I observed:

“The guideline directs me to consider whether the programme involves information matching ‘on a scale that is excessive’ having regard to ‘the amount of detail about an individual that will be *matched* under the programme’. The word ‘matched’ is not defined and I think it makes most sense in this context for the term to mean something like ‘used or disclosed’ rather than simply ‘compared’. For instance, telephone numbers will not be compared in this match but, where there is a hit, IRD will disclose to Courts the taxpayer’s telephone number ... The authorised disclosure of information as a result of the match is an integral part of a ‘matching programme’. It would be quite inadequate for me to judge whether a programme is ‘excessive’ solely on the basis of the details being compared, if as a result of that match, huge quantities of data on individuals are to be disclosed to the matching department in relation to successful hits”.³⁹

- 10.3.12 It would be desirable to refer specifically to the amount of information disclosed as a result of the match. It seems to me that this is consistent with a full examination of whether a programme is “excessive” in scale. I believe it would be desirable for the matter to be considered expressly in this context.
- 10.3.13 Another aspect relevant to whether a match is “excessive” is the frequency of matches. One of the existing matches is operated once each year. At the other end of the scale there is an on-line match which occurs a number of times each day. If frequency is explicitly mentioned in the guideline (e) then departments in their Information Matching Privacy Impact Assessments⁴⁰ will expressly address the question and make their intentions plain. It may be that the departments conclude that an annual or semi-annual match is sufficient as against, say, a monthly or fortnightly match. Where there is a good case for a frequent match this will not, of itself, render it “excessive”. Rather, it is a matter of the frequency being proportionate to the character and objectives of the match.

³⁷ See Report by the Privacy Commissioner to the Minister of Justice on an Examination of a proposal to amend section 126A Social Security Act 1964, August 1997.

³⁸ See Report by the Privacy Commissioner to the Minister of Justice on an Examination of a provision in the Summary Proceedings Amendment Bill (No 3) inserting an information matching provision into the Tax Administration Act 1994, March 1998.

³⁹ *Ibid.*, paragraph 3.5.3.

⁴⁰ The IMPIA process is discussed at paragraphs 3.3.40 - 3.3.42.

**RECOMMENDATION 123**

Section 98(e) should be amended so that in considering whether a programme involves information matching on a scale that is excessive, regard is also had to:

(iii) the amount of detail about an individual that will be disclosed as a result of the programme; and

(iv) the frequency of matching.

Paragraph (f)

- 10.3.14 Guidelines (d) and (f) provide for a proposed programme to be judged against the requirements of the information privacy principles and the information matching rules. However, the controls placed on authorised information matching programs are not simply found in the principles or rules but also in Part X of the Act itself. It would make sense for a proposed matching programme to be examined in advance for its prospective compliance with Part X.
- 10.3.15 I have emphasised in my dealings with departments the need to carefully work through their proposed operating procedures to ensure that there will be no difficulty in compliance with Part X. However, my experience has been that departments have nonetheless got themselves into compliance difficulties which has, in turn, made my job of monitoring compliance with the information matching controls quite difficult.
- 10.3.16 The main example of this, referred to often in my annual reports, has been the inability of the Department of Social Welfare to report to me satisfactorily on the operation of programmes in the manner or detail that it contemplated by section 104. Another example is the operation of the NZ Employment Service-NZ Income Support Service match in which it was discovered after the information matching provision had already been enacted that the departments could not comply with the periods allowed in Part X for the service of notices.⁴¹ A final illustration, concerns one department which continues to debate the need for the notices contemplated by Part X being given in the particular match because it asserts that other safeguards ought to suffice (a point, incidentally, that I do not accept).
- 10.3.17 However, whatever the merits of departmental cases for reporting, serving notices, or giving notices, the point is that any department should make the issue plain, and plead its claimed “special case”, before receiving the authorisation to carry out the match. It is quite unacceptable and inefficient for the match to be authorised and be subject to Part X and only *then* for a department to start raising issues. Departments seeking authorisation for an information matching programme under Part X are, quite sensibly, assumed to know that they will be subject to Part X and it is understood that they will, of course, comply. For the most part that is a sound assumption. However, experience suggests that the matter ought to be made explicit so that programmes will be assessed, in advance, to ensure that they will comply not only with the information matching rules but also Part X.
- 10.3.18 Sometimes departments will seek a dispensation or authorisation within their information matching provision. This should not routinely happen since the scheme of Part X, and the information matching rules, provide a regime for the systematic control of information matching to appropriately protect privacy and meet the needs of other public interests. Nonetheless, there may well be some special circumstances needing, in essence, an exemption from one or more of the information matching rules or perhaps aspects of Part X. If an information matching provision so provides it will likely override a contrary provision in Part X (through the normal rules of statutory interpretation whereby a spe-

⁴¹ See Report of the Privacy Commissioner to the Minister of Justice on the Social Security Amendment Bill, April 1997.

cific provision prevails over a general provision, and a later statute prevails over an earlier one). However, by incorporating reference in information matching guideline (f) to compliance with Part X this can be more clearly taken into account in the examination and authorisation processes.



RECOMMENDATION 124

Section 98(f) should be amended so that the information matching guideline refers not only to the information matching rules but also to Part X of the Act.

10.4 SECTION 99 - Information matching agreements

10.4.1 A written agreement is necessary between the relevant agencies before personal information held by one specified agency may be disclosed, pursuant to an information matching provision, to another for the purposes of an authorised information matching programme. The agreement must incorporate provisions that reflect the information matching rules, or provisions that are no less strict than those rules, and the agencies concerned must comply with those provisions. A copy of the agreement, and any subsequent amendments, must be forwarded to the Privacy Commissioner without delay.

Upside

10.4.2 A clear written agreement between the parties to an information matching programme is also a feature of North American schemes for controlling data matching.⁴² I expect that in those jurisdictions where agreements are not formally required the relevant agencies would, in any case, execute such agreements. An agreement is valuable for a number of reasons and it helps ensure that all parties are aware of their obligations.

10.4.3 Two suggestions for amendment were made to me in the course of consultation. One matching agency advocated the repeal of section 99(3), allowing for the charging of fees for services rendered, on the basis that the matter could simply be addressed between the parties. I take the view that section 99(3) needs to be retained. Without such a provision source agencies might be put in a difficult position in negotiating an agreement to recover their costs. Also, section 99(3) fees provide a convenient starting point, common to all matches, for the examination of the monetary costs of a match.

10.4.4 The other suggestion, made by more than one respondent to the information matching questionnaire, was that information matching agreements should be reviewed periodically by the parties to ensure that they remain relevant. The results should be reported to the Privacy Commissioner even if there is no resultant change to the agreement.⁴³



RECOMMENDATION 125

Section 99 should be amended to require the parties to review any information matching agreement at least once every three years and to report the results of that review to the Privacy Commissioner.

Downside

10.4.5 In some respects information matching agreements add a level of complexity, and potential for confusion, to the scheme provided by Part X and the Fourth Schedule. I expect that it has been intended that the information matching agreements particularise the requirements of the information matching rules and apply them clearly, and in appropriate detail, to the circumstances of a particular match. However, that has not always happened. Sometimes all that

⁴² See, for example, Privacy Act 1974 (USA), 5 USC §552a (o); Treasury Board of Canada Manual, Chapter 2.5 (Data Matching), page 8 (version 1 December 1993).

⁴³ If the agreement itself is changed this must already be copied to the Commissioner under section 99(4).

happens is that an agreement is prepared which paraphrases, and sometimes mis-states, the information matching rules.

- 10.4.6 I have not had sufficient resources to closely monitor the content of information matching agreements and indeed section 99 does not confer upon me any express function in that regard. However, on occasion my staff have compared the relevant clauses in agreements to the corresponding rules and found quite a casual translation of the obligations with, for example, “adverse action” being replaced with simple reference to “action” and “detected” overpayments substituted for “established” overpayments.
- 10.4.7 Even where confusion is not introduced by the substitution of imprecise or inappropriate terminology, the potential benefit of having an agreement is often not achieved. For example, one agreement refers to various obligations being placed with “either party” whereas it is presumably anticipated that an agreement should precisely identify the steps to be taken by, and obligations on, *each* agency.
- 10.4.8 The full potential for problems has not been realised yet due to the limited number of complaints.⁴⁴ I anticipate that there will be complexities uncovered in cases where an information matching agreement is claimed to be relevant in a complaint to an issue of compliance with Part X. It is essential that agencies appreciate the need for the agreements to be suitably detailed and particular.
- 10.4.9 I do not recommend that the role of the information matching agreement be dispensed with at this time. However, I do raise the possibility of problems and encourage specified agencies to give careful thought to the provisions in their information matching agreements. The provision for periodic review by agencies themselves may lead to an improvement in the position particularly as greater compliance experience is gained and shared between agencies. If resources were to be made available, it might be possible to undertake some work with agencies in developing a form of “model contract” which may be suitable for adaptation for particular programmes.

10.5 SECTION 100 - Use of results of information matching programme

- 10.5.1 This section provides that a specified agency that is involved in an authorised information matching programme may take adverse action, as defined in section 97, against an individual on the basis of results produced by that programme. However, this is subject to any other restrictions in law that limit or restrict the information that the agency may take into account in the circumstances.
- 10.5.2 A response to the questionnaire expressed concern that, as presently drafted, the section does not adequately limit who may use the results of an information matching programme. An example would be where a match has been established to enable agency A to take adverse action against individuals in respect of matters for which it is responsible. Agency A sends a list of its clients to agency B which carries out the process of comparison. Agency B returns the list of hits to agency A to enable adverse action to be taken. However, the concern expressed about section 100 was that agency B might not be precluded from itself using the results of the match for purposes of its own.
- 10.5.3 While the matter may not be as clear as might be desirable, I do not fully share the department’s concerns. Generally speaking present information matching

⁴⁴ Persons who have been matched are not usually told by agencies that they may complain to the Privacy Commissioner in the case of a breach of the information matching controls.

provisions have been written sufficiently precisely to make it quite clear what the purpose of the match is and which of the two agencies (or both) may make use of the results of the programme. While clarification would not do any harm, a change does not seem essential to achieve the desired end of constraining use of the results by agencies for which the information is not intended.

- 10.5.4 Section 100 uses the phrase “any specified agency that is involved in an authorised information matching programme”. At present, one cannot ascertain through the Privacy Act itself which agencies are actually involved in a particular programme. It may be that by listing specified agencies in the Schedule against the provisions which apply to them and by incorporating reference to “user agency”, which I have proposed be defined, the suggested problem could be addressed.⁴⁵ The proposed change would make the position plain, and constrain use, without the need to refer elsewhere to the information matching provision in question.

10.6 SECTION 101 - Further provisions relating to results of information matching programme

- 10.6.1 This section provides for certain restrictions on the right to use the results of an authorised information matching programme. Information produced by such a programme must be destroyed not later than 60 working days after the agency becomes aware of a discrepancy produced by the programme unless, before the expiration of that period, the agency decides to take adverse action against an individual on the basis of a discrepancy. Adverse action undertaken by an agency must be commenced not later than 12 months from the date on which the information was obtained by the agency. Where an agency decides not to take adverse action against an individual on the basis of the information produced by a programme, or where the information is no longer needed for such a purpose, the agency must destroy the information as soon as practicable.
- 10.6.2 Several comments in relation to this section were received in response to the questionnaire and discussion paper. It was suggested that the inter-relationship between the time limits in section 101 and information matching rule 6 regarding destruction of information could be better integrated. I suggest that consideration be given, when the information matching rules are more thoroughly revised, to consider how best this might be achieved.

Inland Revenue Department

- 10.6.3 Section 101(5) provides nothing in the section applies in relation to the IRD. Similarly, information matching rule 6(3) provides that nothing in that clause, which concerns destruction of information, applies in relation to the IRD. Accepting for the purposes of discussion that it necessary for IRD to be exempted, it does appear that the exemptions are drafted in a manner which may have a broader effect than was intended. I expect that it was intended that the exemption would apply where the information was supplied to IRD, or the “hits” were supplied to IRD, in order to allow IRD to take taxation-related adverse action against taxpayers. To use the terminology that I earlier proposed be introduced, I believe that the exemption was intended to apply to IRD where it is the authorised “user” agency.
- 10.6.4 I do not imagine that where (again to use the new terminology) a “source agency” supplies information to IRD to match, with the resultant hits being returned to the source agency as the “user agency”, that it was intended that IRD might also retain the list of hits on its records. Unless that is an intended effect of the programme then this should not be allowed to happen and IRD should not be able to use the exemption to permit it to retain the information. If IRD be-

⁴⁵ See recommendations 120 and 121.

believes that it legitimately should be able to use the particular information in the public interest then this should be written into the relevant information matching provision. Under the proposed terminology, IRD should be identified in such cases as a “user agency”.



RECOMMENDATION 126

Consideration should be given to limiting the Inland Revenue Department’s exemptions in section 101(5) and information matching rule 6(3) so that IRD is exempted from obligations to destroy information only where this is an intended objective of the programme.

10.7 SECTION 102 - Extension of time limit

10.7.1 This section provides that I may extend the 60 day time limit set out in section 101, if I am satisfied that the agency cannot reasonably be required to meet it because of the quantity of information obtained through the matching programme, the complexity of the issues involved or for any other reason.

10.7.2 In only one case has an extension of time been sought. The first attempt to run the IRD/DSW Commencement-cessation Match, formerly operated under section 13A of the Inland Revenue Act 1974, encountered difficulties in March 1993. In May 1993, DSW requested an extension of time under section 17 of the Privacy Commissioner Act 1991, the forerunner to section 102, to allow it to keep information generated by the March matching run which might otherwise have had to have been acted upon or destroyed within 60 working days. In the event, before the 60 day limit had expired and before I had made a decision upon the application for extension of time, DSW abandoned the March 1993 match results in the light of a decision to offer a benefit fraud amnesty.

10.7.3 A provision, such as section 102, conferring a discretion to extend time limits, remains desirable. The position seems more satisfactory from a privacy perspective than is the case in the Australian statutory data matching programme in which the relevant departmental Chief Executive can simply grant the extension.⁴⁶ It seems preferable that, if the time limits are to be meaningful, the occasional extensions which may be necessary should be the subject of an application to the independent Commissioner. Section 102 also appears preferable to the Australian approach in that it identifies reasons for which the Commissioner might grant an extension (albeit that the Commissioner can grant extension “for any other reason” in section 102(c)). The Australian provision gives no such guidance.

Which time limit?

10.7.4 One unsatisfactory aspect of section 102 is that it simply refers to extending “the *time limit* set out in section 101” whereas there are two time limits separately identified in that section. There is a 60 day time limit in section 101(1) and a 12 month limit in section 101(2). As mentioned, I have only ever received one application for an extension of the 60 day limit and, in fact, was not required to form an opinion on it. I have never been called upon to provide an extension in relation to the 12 month limit.

10.7.5 I note that section 102 was modelled upon section 10(3) of the Australian Data-matching Program (Assistance and Tax) Act 1990 (with the relevant provision now being contained in section 10(3A) by reason of a 1992 amendment). The Australian provision is directed solely towards the equivalent of the 12 month limit in section 101(2). This may be the period that the drafters of section 102 had in mind rather than the 60 day limit.

⁴⁶ Data-matching Program (Assistance and Tax) Act 1990, section 10(3A).

- 10.7.6 It seems desirable to amend section 102 to make the position plain. It may be desirable to allow the extension power to apply to both time limits even if it was originally only intended that extensions be able to be granted in respect of the 12 month limit. Given present experience, which suggests that applications will be rare, it seems desirable to allow the degree of flexibility that a broad extension power will bring. Nonetheless, I do see the extension power as being relevant to the exceptional cases and not as a means to routinely expand the time frames provided for in the legislation.



RECOMMENDATION 127

Section 102 should be amended to make clear that it refers to both the 60 working day time limit in section 101(1) and the 12 month time limit in section 101(2).

10.8 SECTION 103 - Notice of adverse action proposed

- 10.8.1 Section 103 provides that an agency may not take adverse action against an individual on the basis of a discrepancy produced by an authorised information matching programme, unless the agency has given that individual written notice of the particulars of the discrepancy. The agency must also provide details of the adverse action that it proposes to take and must allow the individual 5 working days from the receipt of the notice in which to show cause why the action should not be taken. There is also provision governing the circumstances in which the notice requirements may be dispensed with and concerning the deemed delivery of notices. The provision is modelled upon similar provisions in the Australian and American laws.⁴⁷

- 10.8.2 The period of notice in section 103(1) is 5 working days. This is provided in order to give the individual a chance to consider the matter and get in touch with the department to explain why it would be wrong to take adverse action. The period is not particularly generous to the individuals concerned and contrasts with the 28 day period (which translates to 20 working days) in the Australian Act.⁴⁸ The period initially specified in the Privacy of Information Bill was 15 working days, already a reduction upon the entitlement in the equivalent Australian legislation.⁴⁹ However, at Select Committee this was reduced to 5 working days. I am not satisfied that the reasons advanced in 1993 for doing so, such as a concern about departments being delayed in taking action, warranted the restriction. Nonetheless, I see no need to adopt a period as lengthy as exists in the Australian legislation. I take the view that 5 working days is too short and the protection of individual rights would be enhanced by modestly extending the period to 10 working days.



RECOMMENDATION 128

Section 103(1) should be amended by substituting a 10 working day period for the present 5 working day period.

Subsection (1A) - the Customs Match

- 10.8.3 Even before the Privacy Act 1993 had come into force it was subject to the Privacy Amendment Act 1993. This amendment inserted section 103(1A) which provides that in respect of the Customs Match the normal 5 day notice is not required. It is interesting to note that a match very similar to the Customs Match is currently being contested in a country sharing a number of values in common with our own. The following extract is taken directly from a recent annual report of the Privacy Commissioner of Canada:

⁴⁷ See Data-matching Program (Assistance and Tax) Act 1990 (Australia), section 11, and the Privacy Act 1974 (USA), 5 USC §552a(p)(3) and (4).

⁴⁸ Data-matching Program (Assistance and Tax) Act 1990 (Australia), section 11.

⁴⁹ Privacy of Information Bill, clause 104.

“Attention now turns to a practice which poses a deadly threat to privacy and to its corollary - autonomy and personal freedom. It has led us into a head-on collision with two great departments of government, HRDC⁵⁰ and Revenue Canada, precipitating a legal challenge which may ultimately determine whether privacy is a fundamental value of this society or merely an irritant quickly to be consigned to the scrap heap of unfulfilled good intentions when the going gets tough.

“That issue is data matching, an innocent-sounding activity with the capacity to demolish any real right to privacy and certainly to destroy the basis of trust which must exist between citizens who provide, and governments which collect, personal information.

“Given the intense pressure on government departments to be leaner (and, if necessary, meaner) coupled with the alluring ease of tracking citizens with computers, a confrontation was probably inevitable.

“At issue is HRDC’s practice of collecting data from the Customs declarations of every returning air traveller to identify employment insurance claimants who were out of the country while receiving benefits. EI⁵¹ claimants must report any extended absence from their normal residence for the good reason that they are expected to be looking, and available, for work. HRDC officials (and many taxpayers) have long been troubled by anecdotal evidence - approaching an urban legend - that many claimants were enjoying holidays at taxpayers’ expense. The department’s administration and enforcement methods were allegedly proving ineffective.

“HRDC conceived the notion of matching the EI database with that of returning travellers’ customs declarations. The match would quickly show whether any of those millions were receiving employment insurance payments. It would then be a simple matter to find whether they had reported their absences.

“Doubtless such a match will catch some who may be cheating EI. But the price it exacts is far too high. It systematically searches millions of innocent travellers, without their knowledge or consent, who filed customs returns on the assumption - and on Revenue Canada’s word - that they would be used for customs purposes only.

“The match offends the most fundamental principle of any privacy law; that government tell its citizens why it is collecting personal information, then use it only for that - and not a wholly unrelated - purpose (unless the individual consents). The reason for the principle is clear: to prevent the government from conducting unwarranted surveillance on its citizens by prowling through its immense personal databanks on what amounts to nothing more than high-tech fishing expeditions.



Bruce Slane and Bruce Phillips: The New Zealand and Canadian Privacy Commissioners confer at the 1998 Privacy Issues Forum.
PHOTO: OFFICE OF THE PRIVACY COMMISSIONER

⁵⁰ Human Resources Development Canada.

⁵¹ Employment Insurance.

“Let us try a pre-computer age analogy. Assume there are some criminals at large in your community. Assume that the police therefore embark on a search of every single household, without warrant, without notice, without permission, and without any cause to suspect any particular household. The police just show up, barge through the door, and look around. How long would any community accept such arbitrary behaviour?”

“Yet, in an information context, that is precisely what data matching makes possible - a systematic search of everyone. Governments which match data this way have turned the presumption of innocence on its head; everyone is suspect until the computer proves them innocent. It is akin to what an earlier privacy commissioner described as ‘high technology search and seizure’. If we allow government to carry on in this fashion, they will routinely scrutinize every record of every citizen until they unearth some evidence of guilt.

“A privacy commissioner cannot accept a data search that ignores the presumption of innocence, the need to identify some reasonable grounds for suspicion, and the absence of independent authorization. If such matches become standard practice, we face virtually open season on any personal information we entrust, or are forced to deliver, to government.

“Unable to convince bureaucrats, or their ministers, to modify the match, we sought legal advice from one of Canada’s leading constitutional experts. His advice buttressed our position that the data match violates the search and seizure provisions of the *Canadian Charter of Rights and Freedoms*. We are currently exploring with the government the most expeditious manner of getting the matter before the Courts for resolution.

“No more crucial issue has arisen in my six years in this Office. I have no more interest in protecting [EI] cheats from detection than the next taxpayer. I have every interest in preventing government from putting millions of law-abiding Canadians under ‘dataveillance’. As a people and a society, we enjoy Charter protection against having to prove our innocence. One’s Charter rights should not be compromised simply because technology makes it possible.

“The premise of this match is boundless - once entrenched, we are on the slippery slope to a general surveillance system in which personal data from all levels of government are routinely shared and matched.”⁵²

- 10.8.4 I earlier noted that Part X has a role in *legitimising* data matching. It is in this context that I have my greatest concern with the Customs Match. Our present privacy law legitimises this programme and yet the Privacy Amendment Act 1993, which inserted subsection (1A) into section 103, undercuts the most fundamental of information matching safeguards - the presumption that the mere matching of information is not sufficient in itself to show guilt and that

⁵² Bruce Phillips, Privacy Commissioner of Canada, *Annual Report 1996-97*, pages 3-5.

the individual should be given an opportunity to explain themselves before adverse action is to be taken. I consider section 103(1A) to be an unjustified inroad into privacy safeguards which undermines the confidence the public ought otherwise to be entitled to have in respect of such an important matching programme.

- 10.8.5 Subsection (1A) also adds an unwelcome complication to the requirements of section 103. It has no application to most of the matches that are undertaken and, even if it were justified, the content of the subsection should really have appeared in section 280 of the Customs and Excise Act 1996. If it were relocated there the effect would substantively be the same but it would not result in clutter in the Privacy Act or confusion for other agencies.
- 10.8.6 However, relocation of the provision is not the best solution. It should, in my view, be totally repealed. It is objectionable in principle and has proved unnecessary in practice. When it was enacted in 1993 the Department of Social Welfare claimed that the amendment was urgent and essential to make the match effective. In fact, the Department has never used it and yet the match has been operated for a number of years. Years after the event, the Department may now wish to start relying upon it. This ought not to be permitted. Dispensing with the fundamental right to be notified of the proposed adverse action was never “essential”. This unjustified inroad into the scheme of information matching controls should be abolished.



RECOMMENDATION 129

Section 103(1A) should be repealed.

10.9 SECTION 104 - Reporting requirements

- 10.9.1 Section 104 provides that a specified agency that is involved in an authorised information matching programme must make certain reports to the Privacy Commissioner in respect of that programme, as may be required by the Commissioner from time to time.
- 10.9.2 In one sense the detail of section 104(2) is unimportant. This is because that subsection is not intended to limit the generality of section 104(1) which obliges agencies to make such reports as the Commissioner may require. However, section 104(2) is important as indicating Parliament’s expectations as to reports which might well be required. It provides a degree of guidance to the Commissioner and agencies. In particular, agencies can use section 104(2) as a guideline when planning the reporting capabilities of their information systems for a new programme.
- 10.9.3 In practically all cases to date it has been expected that agencies would report in the manner contemplated by section 104(2). This will not necessarily always be the case in the future. I would hope, after some years operation of any particular match, that a degree of comfort in relation to the issues addressed in section 104(2)(e) could be achieved allowing the adoption of less detailed reporting. I also hope to explore having departments undertake internal compliance audits with the results only reported to me rather than the “raw data” as contemplated by, say, section 104(2)(e). This comfort zone has not yet been reached with all matches I regret to say.

Australian equivalents

- 10.9.4 The detail of the provision has been derived from similar reporting requirements under the Australian Data-matching Program (Assistance and Tax) Act 1990. Specifically, the provision was modelled upon clause 9 of the schedule to that Act as it existed when the Privacy Commissioner Act was enacted in December 1991. The schedule to the Australian Act has since been supplanted by

a set of guidelines which have themselves been amended. The Australian Privacy Commissioner first issued guidelines pursuant to section 12 of the Australian Act in 1991. These replaced the schedule to the 1990 Act. The current Data-matching Program (Assistance and Tax) Guidelines were issued in 1994 and came into effect in early 1995.

- 10.9.5 The current guidelines do not appear to significantly differ from clause 9 although the following changes may be noted:
- the phrase “matches undertaken”, which is referred to in section 104(2)(e)(i) of our Act, has now been defined;⁵³
 - in relation to the material corresponding to section 104(2)(e) of our Act, the sub-paragraphs which refer to the “number of” items followed by, or preceded by, the “proportion of” such items, have been combined into composite “number and proportion of” provisions;
 - a reference to “successful recovery action” was replaced by a reference to “cases where the debt was fully recovered” perhaps to clarify what constitutes “success” - the nearest equivalent in our Act is section 104(2)(e)(viii) which refers to the number of “successful” cases but which, due to the broader coverage of the Act, is not described solely in terms of recovery action.
- 10.9.6 One of the responses to the questionnaire offered some criticisms of section 104(2)(e). The respondent pointed out, for example, the link between paragraphs (ii) and (iii), and (iv) and (v) which call for both figures and proportions while noting by contrast that (vi) and (viii) call only for a number and (vii) only for a percentage. The same respondent pointed out that (viii) refers to the number of cases - but not value - in which action taken was “successful”. It was suggested that value was important in constituting “success”. Consideration should be given to adopting some of the changes that have been made to the Australian provision from which section 104 has been derived. The Australian provision seems to have a more satisfactory current structure.



RECOMMENDATION 130

Consideration should be given to amending section 104(2)(e) to adopt aspects of the clause 12(v) of the Australian Data-matching Program (Assistance and Tax) Guidelines.

10.10 SECTION 105 - Information matching programmes to be reported on in annual report

- 10.10.1 Section 105 requires me to report on each authorised information matching programme in my annual report.
- 10.10.2 This has caused me some difficulties with completing my annual report, under section 24 of the Act, in time. I have been delayed in submitting my annual report because of the need to await departmental reports on the last matching runs held during any financial year in respect of particular information matching programmes. Consequently, the report on my activities tends to get held up which places me in the embarrassing position of failing to meet the timetable imposed by the Public Finance Act 1989 for the tendering of annual reports or failing to comply with this section. For example, in the 1996/97 year, final reports for four important matching programmes were only received by 22/23 September 1997.⁵⁴ In addition to the delay in completing the section 24 report, the need to finalise and submit my general annual report means that the

⁵³ Guidelines, clause 2.2(e). The definition is as follows: “**matches undertaken** refers to the total number of records received by the matching agency from assistance agencies after they have been separated into individual records for clients, partners, children, parents, maiden names and aliases.”

⁵⁴ These concerned the IRD/DSW Commencement/cessation match, Education/DSW match, Customs/DSW match and Corrections/DSW match.

report on information matching often has to be finalised in haste after the last departmental matching reports are to hand.

- 10.10.3 The two types of annual reports differ in nature and I believe there is a good case to split the reporting requirements. The section 24 report is an account of the activities of my office. The section 105 report is primarily, although not exclusively, a commentary upon the activities of other agencies. From a practical point of view, the completion of the section 24 report is within my own hands whereas I am dependent upon other departments to enable me to complete an adequate section 105 report.
- 10.10.4 I have considered several options for addressing the problem. The first would be to continue, as now, to try to reconcile the competing demands by allowing the section 24 report to be rather late and to complete the section 105 report as quickly as possible once the reports are to hand. However, this places me at risk in relation to compliance with the Public Finance Act. I have considered as an option whether to simply submit my annual report when the section 24 material and audited accounts are to hand, regardless of whether a complete set of departmental information matching reports are available to comment upon. I am reluctant to do this since it may mean that Parliamentary and public scrutiny of some of the matches, particularly those which have most difficulty in meeting section 104 reporting requirements, will be diminished. Furthermore, I am uncomfortable with failing to deliver a complete assessment of each information matching provision as anticipated by section 105. A third option was to adopt a different reporting year under section 105 to that used in the rest of my annual report and generally in the public sector. This would have the “information matching” year finish on, say, 31 December or 31 March. I concluded that this would be confusing.
- 10.10.5 Accordingly, I decided that the best way of resolving the problem will be to sever the section 105 report from the section 24 report. This will require section 105 to be amended since it anticipates the information matching report to be included “in every annual report of the Commissioner” which clearly refers to the section 24 report. Although I cannot be precise as to when an information matching report would likely appear each year I anticipate that it would usually be a few months after my general report. My annual report tends to be ready by about September each year and the information matching report could usually be ready by December. As with the present arrangement, I would wish the annual report to be tabled in Parliament since my recommendation is not intended to be a substantive change merely an alteration in timing and presentation. I suggest that the section merely provide that there be a report in terms of section 105 in respect of each year or, if it is desired to be more precise about the timing, that the report be submitted “as soon as practicable” following the completion of any year.



RECOMMENDATION 131

Section 105 should be amended so that the annual information matching report may be submitted separately from the annual report required under section 24.

Costs of monitoring and assessment

- 10.10.6 Section 105(3) provides that for the purpose of carrying out any assessment required to establish a programme’s compliance with Part X and the information matching rules that the provisions concerning complaints and investigations apply as if the assessment were an investigation under Part VIII of the Act. This anticipates more rigorous compliance assessments than has been possible for me to undertake to date. Primarily, the assessment that I have made to date have been done on the basis of an examination of the reports submitted to me under section 104 supplemented by specific correspondence. While I, and my staff, from time to time meet and talk with staff of agencies involved in infor-

mation matching I have not inspected premises with a view to making an assessment of the extent of any programme’s compliance.

- 10.10.7 This contrasts with the Australian Privacy Commissioner’s office which has been active in efforts to assess compliance. The Australian Commissioner’s Information Technology Standards Section monitors the statutory data matching programme by conducting audits of procedures and practices that are in place in the agencies.⁵⁵
- 10.10.8 The Act contains sufficient powers for me to undertake a more active role in this regard. Unfortunately, on present resources and particularly with the competing priority of a 12 month complaints queue, it has not been feasible to undertake such work. An independent oversight body in respect of data matching is intended to give the public, and affected individuals, some confidence that someone other than the agencies involved in the programme is ensuring compliance with the law. However, on present resourcing I fear that public confidence in the degree of oversight may be somewhat misplaced. This is compounded by the fact that reliance has been placed on the reports given to me under section 104 and experience has shown that the data contained in those has, in some cases, been wildly unreliable.
- 10.10.9 It may be appropriate to require specified agencies to fund the Privacy Commissioner to carry out aspects of this oversight role. This may seem appropriate for the following reasons:
- the extent of the work involved depends upon the number of new matches authorised and the amount of matching activity undertaken - the increase in the number of matches authorised has increased the work for my office;
 - enhanced activity by my office in respect of information matching will have a positive effect for agencies in helping them comply with the Act;
 - there is a benefit to specified agencies in being able to reassure the public that the process is carried out in the way which respects individual rights - the existence of independent oversight can help dispel public concerns about the process;
 - present arrangements mean that the cost of appropriate oversight are hidden, whereas it should be seen as one of the component costs of every authorised information matching programme.
- 10.10.10 My proposal has something of the “polluter pays” principle about it. The agencies which carry out the privacy intrusive process should bear the costs of the regulation which reassures the public, and Parliament, that citizens rights are being appropriately protected and the programmes are being carried out in the way that the legislation anticipates. This principle has already been accepted in Australia where the Commonwealth Department of Social Security provides funds to the Australian Privacy Commissioner for data matching regulation. The total amount received in 1996/97 was \$333,000.⁵⁶ If the Act adopts the concepts of “source agency”, “matching agency” and “user agency” it will be possible to most equitably allocate costs rather than levying all specified agencies equally. Costs would mainly be directed towards matching/user agencies.



RECOMMENDATION 132

Consideration should be given to funding the Privacy Commissioner’s information matching monitoring activities by charges on specified agencies involved in carrying out information matching programmes.

⁵⁵ See Australian Privacy Commissioner, *Ninth Annual Report*, 1996/97, page 102.

⁵⁶ *Ibid*, page 113.

10.11 SECTION 106 - Review of statutory authorities for information matching

10.11.1 Section 106 requires me at periodic intervals to review the operation of every information matching provision and to consider whether or not, in my opinion as Privacy Commissioner:

- the authority conferred by each information matching provision should be continued; and
- any amendments to the provision are necessary or desirable.

10.11.2 After a belated start, I have commenced work on this review. It has been necessary in 1998, as a matter of priorities, to delay completion of the first stage of the section 106 review as resources were deployed on completing this review. However, the section 106 review has progressed sufficiently such that the first part of that review should be complete at a time not too distant from the submission of this report.

10.11.3 If one considers the controls in Part X of the Privacy Act as following each part of an information match's life cycle the process might be characterised as:

- *authorisation* - the processes and controls which determine whether a proposed match should proceed and in what manner;
- *operation* - controls to ensure that privacy risks are minimised, decisions are based upon reliable information, individuals have an opportunity to explain themselves and if necessary complain, and independent oversight of the results of the programme;
- *evaluation* - periodic review of the continuing value of a match in the light of experience and current circumstances.

10.11.4 The section 106 review would encompass the third category. However, it would not be undertaken in isolation from the first two. In evaluating a programme I would look back to the objectives set, and projections made, when each programme was first authorised. I would also study the experience of each match in operation.

10.11.5 Notwithstanding the delay in completing the first batch of reviews expected under section 106, I consider the provision to be of significant importance in the scheme of information matching controls. No amendment to the section appears necessary although the matter could be considered again when the first reviews are complete.

10.12 SECTION 107 - Amendment of information matching rules

10.12.1 This section provides that the Governor-General, by Order in Council, may amend the information matching rules set out in the Fourth Schedule or may revoke the schedule and substitute a new schedule. No Order of this type may be made otherwise than in accordance with the recommendations of the Privacy Commissioner.

10.12.2 No Orders in Council have been made. I consider that the provision ought to be retained since proposals, when they arise, might be expected to be of a technical nature, rather than of a type raising important policy issues, and therefore better suited to regulations rather than requiring Parliamentary time. Nonetheless, there is an important safeguard in that no Order in Council may be made except in accordance with recommendations of the Commissioner. In the event that the Government wished to make a change which the Commissioner opposed, it would be possible for amending legislation to be brought to the House. Parliament would have an important role in respect of such a pro-

posed change. Most submissions saw the present process for amendment by Order in Council as satisfactory.⁵⁷

10.12.3 The information matching rules themselves are set out in the Fourth Schedule. I make some proposals for change to the rules which could be taken forward as part of any amending legislation arising from this report or separately by way of Order in Council. The changes that are proposed are relatively modest. A more thorough review of the information matching rules than has been possible on this occasion would be desirable with amendments made, as a result, by way of the section 107 process. This might usefully await the Government's responses to my recommendations for amendment to Part X. The Australian Privacy Commissioner has recently completed a revision of the relevant guidelines which may also present issues worth special consideration.⁵⁸

10.12.4 The changes to the information matching rules I suggest below are simply small technical changes which have been brought forward in the course of the review through responses to the information matching questionnaire, submissions on the discussion paper, or as suggestions from staff or agencies. They do not constitute a detailed reformulation of the rules and consideration has not been given at this stage to establishing any new rules. The changes therefore amount to refinement pending a more thorough review or reformulation at a later date.

Rule 1 - Notice to individual affected

10.12.5 Rule 1 obliges agencies involved in authorised programmes to take all reasonable steps (which may consist of or include public notification) to ensure that the individuals who will be affected by the programme are notified of it. This is quite different to the notice of adverse action to particular individuals whose information has been matched. Rule 1 requires specific classes of people to be made aware of the operation of a programme.

10.12.6 This requirement is a manifestation of the OECD "openness principle" which states:

"There should be a general policy of openness about development, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purpose of their use, as well as the identity and usual residence of the data controller".⁵⁹

It is a basic feature of privacy protection that there should be an openness about information use. This is particularly the case with information matching which is an intrusive process of mass "dataveillance" and which anticipates the use of information for a purpose other than that for which it was obtained.

10.12.7 In addition to the benefits for privacy from openness, there is in nearly all cases an incidental benefit to the primary purpose of matches. Many existing matches involve detecting unlawful behaviour. The government's interests will be better served if such wrongdoing is deterred in the first place. Deterrence ought to be underscored by fulsome compliance with information matching rule 1.

10.12.8 It is therefore disappointing to note that agencies have not been as active in

⁵⁷ Submissions PQ3, PQ4, PQ5 and PQ11 saw the process as satisfactory. PQ6 queried whether the process allowed sufficient consultation with affected government agencies while PQ8 considered the rules important enough to require statutory amendment in the rare circumstances that change were to be needed.

⁵⁸ See Australian Privacy Commissioner, *The Use of Data Matching in Commonwealth Administration Guidelines*, February 1998.

⁵⁹ OECD Guidelines, clause 12.

"The use of an Order in Council to amend the privacy rules provides flexibility but also limits the opportunity for other government agencies to comment on the particular amendments. Legislating for changes to the Act provides a greater opportunity for comment."

- INLAND REVENUE DEPARTMENT,

SUBMISSION PQ6

their efforts to publicise the operation of matches as I believe is anticipated by rule 1. Only a few agencies have done a good job of publicising their programmes. Some others have made very expensive efforts from time to time, occasionally using television advertising, but have not sustained the effort at other times. In particular, the opportunities to communicate directly with beneficiaries, upon renewal or at regular intervals, should be taken as such efforts are better directed than mass media advertising.

- 10.12.9 When the information matching rules are more thoroughly revised I suggest that consideration be given to more fully articulating the steps which might be appropriate in notifying the commencement and the existence of a programme and generally making individuals aware of it. The Australian Privacy Commissioner's recently revised guidelines offer some suggestions for study in this regard.⁶⁰ I suggest that the phrase "openness and public awareness" appear in the heading so that agencies are directed to the purpose of the obligation.



RECOMMENDATION 133

Information matching rule 1 should be retitled "Openness and public awareness concerning operation of programme" and consideration should be given to enhancing the rule by detailing mandatory requirements, and a variety of discretionary methods, by which agencies may ensure that individuals who will be affected by a programme are made aware of its existence and effect.

Rule 2 - Use of unique identifiers

- 10.12.10 Rule 2 prohibits the use of unique identifiers in an information matching programme except as provided for in any other enactment or "unless their use is essential to the success of the programme." A perennial problem with information matching is to spot and ensure that the entries in two different databases indeed relate to one and the same individual. If the two sets of data which are to be matched in the programme both contain what should be the same unique identifier, then some would argue that its use may well aid in ensuring that it is the same individual in each database.
- 10.12.11 However, there are reasons which militate against the use of unique identifiers in information matching programmes. Experience has shown that unique identifiers which are held by an agency other than the one which assigned them are frequently incorrect. Thus when asked for their tax file number, some people will deliberately or mistakenly give a number which actually belongs to another member of their family or the agency may simply slip up in transposing the number from one form to another because there is no internal check on such identifiers and one identifier looks much like another. Reliance upon unique identifiers in such circumstances can reduce accuracy rather than increase it.
- 10.12.12 Another, and perhaps and even more compelling, reason for constraining the use of unique identifiers in information matching is the fear that if permitted to be used there will be a very strong incentive amongst Government bureaucracies to encourage the widescale use of shared unique identifiers. This in turn may lead to a national ID number to further facilitate widespread data linkages. Support for the view has been given by a policy decision to encourage the use of the driver licence for secondary purposes.
- 10.12.13 It should be noted that rule 2 is not an absolute prohibition on the use of unique identifiers. It is plain that unique identifiers can be used in two circumstances:
- where their use is provided for in another enactment; and
 - where their use is essential to the success of a programme.

⁶⁰ Australian Privacy Commissioner, *The Use of Data Matching in Commonwealth Administration Guidelines*, February 1998, clauses 33-41.

In fact, unique identifiers feature in several existing information matching programmes.⁶¹

10.12.14 In practice to date, the information which is disclosed for an information matching programme has usually been detailed in the information matching provision. Thus rule 2 has not actually been an impediment to matching agencies so far so long as they can make a case for the unique identifier when they seek legislative authority. In the absence of legislative provision there seems to be no obvious way, short of seeking a declaratory judgment in the High Court, to establish whether or not an agency is correct in a claim that the use of a unique identifier is essential for the success of a programme. I expect that in case of disputes a department might seek to resolve such an issue by having an information matching provision amended to allow expressly for disclosure and use of the unique identifier.

10.12.15 However, it might be desirable to establish a process whereby an agency could apply to the Privacy Commissioner for approval to use a unique identifier where the Commissioner is of the opinion that the use of the identifier is essential to the success of the programme (or some other suitable or additional criterion). The power for the Commissioner to grant approvals under information matching rule 3 may offer a suitable precedent and such a power could provide that the Commissioner may impose conditions on the granting of such approval and may withdraw the approval or vary the conditions at any time. It might be appropriate for the Commissioner to limit approvals to cases where the unique identifier is one that is already assigned by the agencies so as to discourage the spread of common identifiers or the undermining of principle 12.

10.12.16 In the discussion paper I sought views on whether the use of unique identifiers should be permissible with the approval of the Privacy Commissioner. Although some of the replies were ambiguous it appears that nine submissions supported the proposition⁶² while three opposed it.⁶³



RECOMMENDATION 134

Information matching rule 2 should be amended by deleting the phrase “unless their use is essential to the success of the programme” and replace it with provision for agencies to apply to the Commissioner for approval to use unique identifiers where the Commissioner is satisfied that their use is essential to the success of the programme.

Rule 3 - On-line transfers

10.12.17 The prohibition on transfers by on-line computer connections has been derived from the Australian Data-matching Program (Assistance and Tax) Act 1990 which states:

“Data not to be sent on-line

Data is not to be transferred between agencies in the data matching program by on-line computer connections.”⁶⁴

10.12.18 I understand that this total prohibition has been controversial in data matching circles in Australia. Agencies involved would like to have the prohibition lifted and I understand that the Federal Privacy Commissioner has supported their case. However, Parliamentarians have been unwilling to allow that to happen and have apparently voted down a proposed amendment to lift the prohibi-

⁶¹ The tax file number is utilised in five information matching programmes. The Department of Social Welfare number and NZ Employment Service number are jointly utilised in a further match.

⁶² See submissions PQ1-PQ5, PQ7, PQ8, S36 and S42.

⁶³ See submissions PQ6, PQ11 and S45.

⁶⁴ Data-matching Program (Assistance and Tax) Act 1990 (Australia), section 8.

“It will not be possible to use on-line transfers, which are prohibited under the rules. Nor will it be possible to establish a new databank for any matched information. The rules also require information that does not reveal a discrepancy to be destroyed forthwith. The Government is satisfied that this structure will provide the necessary safeguards.”

- HON. DOUGLAS GRAHAM, MINISTER OF JUSTICE, SPEAKING ON THE INTRODUCTION OF THE PRIVACY OF INFORMATION BILL, 1991

tion. It must therefore be acknowledged that at least in Australia there are strongly held views concerning the practice.

10.12.19 I suspect that the concerns exist on three levels. The first relates to the security of transmission of data. There are special information security issues about transfer of data by on-line computer connections but it appears that these are known and understood and able to be addressed. It is by no means certain that physical transportation of tapes and disks is invariably a more secure means of transfer. At the second level, the concerns relate to a fear of the inter-connection of a variety of Government databases. This raises the spectre of a “Government Super-computer” or “Big Brother” database which has been a recurrent public fear manifested in democratic societies. In New Zealand, similar concerns were at least part of the reason for the enactment of the Wanganui Computer Centre Act 1976. Finally, the third set of concerns relate to a worry that incorrect data from either agency be imported into records with insufficient checking in advance or ability to verify after the event.

10.12.20 In my view, there is a case to transfer data by means of on-line computer connections on occasion. Rule 3 is not the absolute prohibition that has been found to be problematic in the Australian legislation.⁶⁵ Agencies may obtain approval from me for on-line computer connections and in respect of one match I have granted such approval (on three separate occasions, the latest taking the approval through to 1 October 1998).⁶⁶ In my view, the rule at present continues to serve a useful function and contains sufficient flexibility to allow on-line computer connections in appropriate cases.

10.12.21 Further study could be given to dropping the prohibition when the rules are more fully reviewed. It may be that it should be replaced with a rule, or rules, specifically tailored to on-line issues. This may be especially desirable given that several of the rules have been originally drafted in Australia with only tape-to-tape matching in mind and may need to be modified to work well with on-line matching.

Rule 4 - Technical standards

10.12.22 There have been problems on occasion with agencies being unable to produce reports to the Privacy Commissioner of the type anticipated under section 104. The suggestion was made in a response to the questionnaire that it might be worthwhile to include in the rules a reference to adequate proposed procedures to generate, and supply, reports which may be required under section 104 by the Privacy Commissioner. Such an obligation would then have to be reflected in information matching agreements, pursuant to section 99 and the matter would therefore be one to which agencies will clearly turn their mind at an early stage and at a senior level. However, my recommendation to amend section 98(f) may diminish the problem and therefore I have not adopted this proposal.

Rule 5 - Safeguards for individuals affected by results of programmes

10.12.23 One respondent to the questionnaire echoed sentiments of others when he suggested that rule 5 was “difficult to understand, possibly ambiguous, and meriting review and revision”. One source of confusion are several difficult concepts such as:

- “the validity of discrepancies” - rule 5(1); and
- “the information which formed the basis for the information” - rule 5(3).

⁶⁵ When introduced in the Privacy of Information Bill did contain an absolute prohibition. The Select Committee introduced the power for the Commissioner to grant authorisations.

⁶⁶ See approval by the Privacy Commissioner under Information Matching Rule 3(1), 1 March 1998. This approval relates to a match operating between NZ Income Support and the NZ Employment Service.

“The other difficulty that I have is perhaps a rather strange one. We have to have a very careful discussion about the banning of on-line transfers, which are prohibited by the third information matching rule. I am not convinced that properly controlled on-line transfers are not a legitimate exercise in terms of, say, matching Department of Social Welfare and Inland Revenue Department data, because we will tend to end up with a much more expensive and highly complex set of manual information exchanges simply so that we can say that we are not having on-line transfers.”

- DR MICHAEL CULLEN, SPEAKING ON THE INTRODUCTION OF THE PRIVACY OF INFORMATION BILL, 1991

“Rule 7 is a valid precaution. Errors of mismatched information can have dire consequences and should not be used to form a new databank.”

- NZ ASSOCIATION OF SOCIAL WORKERS AOTEAROA, SUBMISSION
PQ 4

10.12.24 The origin of rule 5 is clauses 5.1 and 5.2 of the Schedule to the Australian Data-matching Program (Assistance and Tax) Act 1991.⁶⁷ However, the Australian provisions do not carry the two problematic phrases just mentioned. The manner in which they deal with the matter might suggest some ways forward to simplify the provision while retaining its effect. For example, in the Australian guidelines:

- the equivalent obligation to rule 5(1) applies to “source agencies” instead of, “the agencies involved in an authorised information matching programme” - there may be scope for simplification and precision through use of the new terminology suggested elsewhere;⁶⁸
- the phrase “source data”, a defined term, is used instead of “the information which formed the basis for the information” - which may be an approach able to taken up if the rules are used for defining terms as well as laying down rules, as recommended elsewhere;⁶⁹
- the phrase “believed that such results are not likely to be in error” is used instead of “confirming the validity of discrepancies” - I am not saying that one phrase is necessarily better than the other, simply that the Australian guidelines offer an alternative to consider.

10.12.25 The present heading for this clause is not particularly informative. It refers to “safeguards for individuals affected by results of programmes” which could just as easily refer to aspects of many of the other rules. Indeed, it appears that the adoption of that title may have been somewhat inadvertent when carried over from the Australian Act. The Australian Act uses “safeguards for individuals affected by the results of programmes” as a general heading which applies to the equivalent of rules 5, 6, and 7 of our Act. In fact, the precise heading applied to the equivalent of rule 5 in the Australian legislation is simply “fairness”. However, the way in which the heading and subheading are laid out in the Schedule to the Australian Act is confusing whereas the matter has been made much plainer in the Australian Privacy Commissioner’s guidelines. I suggest that a better heading should be adopted such as “procedures for confirming the validity of discrepancies” or “checking results before use”.



RECOMMENDATION 135

A more informative heading should be given to information matching rule 5 and consideration should be given to redrafting the rule in a clearer fashion possibly drawing upon the Australian approach and using defined terms.

Rule 6 - Destruction of information

10.12.26 Some aspects of this rule have been discussed already, at paragraphs 10.6.2 - 10.6.4, in relation to section 101.

Rule 7 - No new databank

10.12.27 One of the perceived dangers of information matching is that, unless action is taken to verify that an apparent match is a true match (that is, that the two records do in fact relate to the same individual), misinformation is generated and may potentially be used in the future upon the unwarranted assumption that the information is a historical fact. Rule 7 prohibits an agency from using the results of an authorised information matching programme to create a new databank and this might be thought primarily to ensure that the unverified information is not later treated as a fact.

10.12.28 It may also be the case that a match produces a “true match” of accurate information but nonetheless a permanent database of the information should not be

⁶⁷ Now contained in the Australian Privacy Commissioner’s Data-Matching Program (Assistance and Tax) Guidelines, clauses 5.1 and 5.2

⁶⁸ See recommendation 121.

⁶⁹ See recommendation 137.

retained. For example, if a superannuitant goes to Australia for a holiday that will be recorded as a departure. When he comes back after two months that is recorded as an arrival. He is within the permitted period of absence and no action needs to be taken. Nonetheless, through the operation of the information matching programme his details are identified. The Department has got the right person who did in fact do the things that the match identified. However, there was nothing wrong with it. It would seem unnecessary and improper to maintain a record of that permanently in Government files. Similarly, an unemployed person goes to Australia to seek a job. In fact she has the approval of the local Income Support office to do so. That record does not find its way through to the Head Office records by the time that the match is run. It is no doubt the right person identified in the particular case. A later investigation shows that she did have the necessary approval. Why should a record that she went to Australia and then came back again be maintained permanently? Accordingly, in addition to the concern about permanent records of misleading results, there is also a desire not to retain permanent databases of information for which no purpose, in terms of taking adverse action against the individual, exists.

- 10.12.29 The agency can keep a register showing those individuals in respect of which a “discrepancy” has been indicated by the matching programme but can only show the minimum details necessary for investigating and taking the adverse action against them. Similarly, the agency can keep a register showing individuals who are to be excluded from further investigation, but again just the minimum amount of information necessary for that purpose. These limitations do perhaps mean that extra work has to be undertaken in some matching programmes because intermediate match information which was not sufficient to warrant adverse action last time is lost and has to be produced again. On the other hand, one can argue that if the information was insufficient to warrant adverse action why should it be retained?
- 10.12.30 Some debate about rule 7 was engendered in the review process in the questionnaire responses and in submissions (for example, submission PQ 2). A suggestion was made to delete the word “permanent” from rule 7(1) and also the word “separate”. This would direct the rule towards avoiding creating new registers or databanks of information and not simply those that are separate or permanent. That idea may have merit but I prefer not to adopt it at this stage pending a more thorough review of the rules. Most submissions supported the rule as a safeguard.⁷⁰

Rule 8 - Time limits

- 10.12.31 I have observed elsewhere that the heading for this rule is somewhat misleading and suggest that it be retitled “Annual frequency of matches”.⁷¹
- 10.12.32 An interesting feature of this rule is that the time limits, or as I would characterise it the frequency of matches, are to be stated in writing in an annex to the Technical Standards Report. It is not plain why the frequency is required to be stated in an annex rather than the technical standards report itself. Indeed, a number of the Technical Standards Reports submitted to the Privacy Commissioner have not bothered to make the distinction. It may have been anticipated that the frequency of matching would likely have been a matter subject to change more frequently than the balance of the Technical Standards Report and that by dividing the material the documentation, and the management of change, may have been more easily handled. The Privacy Commissioner may pursuant to rule 4(6), require a change to a Technical Standards Report. Perhaps the annex was meant to be outside the scope of the Commissioner’s power to vary? If so, the effect is not plain.

“The no new databank rule may frustrate the objectives of matching programmes that have an intelligence gathering function but one can argue if the information was insufficient to warrant adverse action why should it be retained?”

- PAUL KELLY, SUBMISSION PQ2

⁷⁰ See submissions PQ1, PQ3-PQ5, PQ8, PQ11, S36 and S42. Submission PQ6 did not support the rule.

⁷¹ See recommendation 2.

- 10.12.33 In my view, the reason for specifying time limits in an annex is unclear both as to its purpose and effect. I suggest that the distinction be discontinued or, if on further study a good reason is ascertained, that the effect be more clearly spelt out.



RECOMMENDATION 136

Information matching rule 8(2) should be repealed or, if retained, its purpose and effect made plain.

Defining terms

- 10.12.34 The Fourth Schedule may have a useful role to play in defining technical terms which are used in the information matching rules or may be used in the future. However, it occurs to me that the process for amending the Fourth Schedule by Order in Council offers potential not only for defining terms used in the schedule but also for terms used in Part X. This would provide an appropriate way in the future of providing certainty on some legal, technical, and operational aspects without the need to await statutory amendment or to tie up Parliamentary time in enacting matters which may be highly technical.
- 10.12.35 I have seen an example of something similar happening in the Australian environment. Essentially the schedule to the Australian Data-matching Program (Assistance and Tax) Act has been replaced by a set of guidelines issued by the Privacy Commissioner. While the process differs from that provided in our Act, the nearest equivalent would be the issue of a substitute Fourth Schedule by Order in Council under section 107. Those guidelines introduced three new definitions which have not previously appeared in the Act: “Dispute”, “matches undertaken” and “final completion of the action”. “Matches undertaken” is a phrase used in Part X of our Act.
- 10.12.36 Without any amendment to section 107 it would be quite possible for newly issued information matching rules to contain a set of definitions of terms used in those rules. It would not be possible for the rules to define any term that is already defined in section 97 in a way that differs from section 97. Further, in the absence of a specific power to do so in section 97, it would be questionable as to whether the rules could purport to define a term used in both Part X and the rules (or if that was done, it would be unclear whether the definition was binding in respect of Part X itself) or used solely in Part X (which would be highly doubtful). I suspect that, if the Order in Council procedure is to have most value as a definitional aid, section 97 or section 107, or both, should be amended to expressly so provide. The basic power could perhaps be provided in section 107 with section 97 appropriately amended to make clear that any terms not defined in section 97 itself to have the meaning ascribed by definitions (if any) in the information matching rules.



RECOMMENDATION 137

Provision should be made for terms used in Part X, and the information matching rules, to be able to be defined in the information matching rules themselves.

10.13 SECTION 108 - Avoidance of controls on information matching through use of exceptions

- 10.13.1 Section 108 provides that nothing in information privacy principles 2(2)(d)(i) or 11(e)(i), which allow a public sector agency to collect or disclose personal information in order to avoid prejudice to the maintenance of the law, permit the agency to collect or disclose that information for the purposes of any authorised information matching programme, or any information matching programme the object of which is similar in nature to any authorised information matching programme.

- 10.13.2 Where there is a specific statutory arrangement for matching under an information matching provision listed in the Third Schedule, the exceptions to principles 2 and 11 in relation to the maintenance of the law cannot be invoked in order to avoid the controls placed on the authorised information matching programme by Part X. The purpose of section 108 is to counteract a means by which public sector agencies might otherwise be able to circumvent the controls on information matching.
- 10.13.3 Clearly the exceptions to principles 2 and 11 mentioned in the section are the most likely to have been cited in the event that section 108 had not existed. However, they are not the only ones and there is now a broader range of programmes that have been authorised than was the case when section 108 was enacted. For example, there is a match authorised involving the Department for Courts designed to obtain new address information to enable the Department to enforce fines. The harm to which section 108 is directed would also exist if such a department could skirt the information matching controls by reliance upon principle 2(2)(d)(ii) or principle 11(e)(ii) rather than the subparagraphs presently mentioned in the section. The Australian Privacy Commissioner, who has a similarly worded disclosure principle, has also expressed concern at the use of such exceptions to legitimise bulk disclosures for data matching exercises.⁷²
- 10.13.4 Accordingly, I suggest that section 108 be amended to refer to all of the exceptions appearing in information privacy principles 2 and 11.

**RECOMMENDATION 138**

Section 108 should be amended to replace the reference to “subclause (2)(d)(i) of principle 2 or paragraph (e)(i) of principle 11” with a reference to all of the exceptions to principles 2 and 11.

10.14 SECTION 109 - Avoidance of controls on information matching through use of official information statutes

- 10.14.1 Section 109 provides that a public sector agency is not to disclose personal information in response to a request made by another public sector agency under either of the official information statutes where the sole or principal purpose for the request of the information is so that it may be used in an information matching programme.
- 10.14.2 The purpose of section 109, like section 108, is to counteract a means by which public sector agencies might otherwise be able to circumvent the controls on information matching provided for in Part X. However, section 109 goes beyond section 108 in applying to all information matching programmes, not just authorised information matching programmes or programmes which are similar in nature to an authorised information matching programme.

⁷² Australian Privacy Commissioner, *Privacy Protection in the Private Sector: Response to Discussion Paper* issued by the Attorney-General, December 1996, page 9.

Part XI

XI

Law Enforcement Information

337

“Hailed as a beacon at the time of its enactment in 1976, the Wanganui Computer legislation was simply not geared to cope with the broader spectrum of privacy issues that arose during the years that followed. Those issues went far beyond the scope of such a limited statute as the Wanganui Computer Centre Act 1976 and had already drawn a response from the New Zealand Government when it signed the ‘guidelines agreement’ in Rome as far back as 1980. The new Privacy Act is an endorsement of that response.”

- P L Molineaux, *Final Report of the Wanganui Computer Centre Privacy Commissioner*, 1993

“Part XI of the Act and the Fifth Schedule should be retained. They represent a balance between the spirit and intention of the Privacy Act and the needs of an efficient criminal justice system by allowing on-line access to information where it would not be practicable to process individual requests for information because of the volume of cases involved. The Fifth Schedule also has the potential to act as an aid to transparency and accountability in terms of the information handling practices of justice sector agencies.”

- Ministry of Justice, submission H14

“The Group favours a principled and flexible approach as opposed to a prescriptive approach. Part XI of the Act and the Fifth Schedule should be repealed.”

- NZ Law Society Privacy Working Group, submission H15

“The Ministry does not consider the repeal of Part XI and the Fifth Schedule to be practical. It is impossible to assess whether each on-line collection or disclosure of information fits within one of the exceptions to the information privacy principles. It is only practically possible to assess types or classes of information.”

- Ministry of Transport, submission S58

11.1 INTRODUCTION

11.1.1 Part XI makes special provision for certain law enforcement information. It incorporates, in a modified form, the Schedule to the Wanganui Computer Centre Act 1976 which was repealed by the Privacy Act.

11.1.2 The purpose of Part XI was described in the explanatory note to the Privacy of Information Bill as follows:

“The purpose of Part XI is to authorise access by certain

Government departments and local authorities to law enforcement information stored by other Government departments on the Wanganui computer. In the absence of this authority, access that is available now might not be permitted under the Bill because it would not otherwise be permitted by the information privacy principles. It was considered preferable to continue in a modified form the provisions of the schedule to the Wanganui Computer Centre Act 1976 rather than provide wide exceptions to the information privacy principles in order to preserve such access.”

11.1.3 Although Part XI, and its associated schedule, were carried forward into the Privacy Act 1993 as enacted, the Select Committee did make certain changes. As outlined below, one of those changes - concerning the method of amendment to the schedule - has been brought forward as a significant issue in the review.

11.1.4 In reviewing Part XI and the Fifth Schedule, it has been necessary to consider, amongst other things:

- whether the purpose of Part XI, as described above, was indeed an appropriate approach to the issue of law enforcement information sharing;
- whether the process for amending the Fifth Schedule, introduced by the Select Committee, should continue;
- what method of amendment to the Fifth Schedule should be adopted if change is to be made;
- how well Part XI and the Fifth Schedule have met the challenges of justice sector reorganisation, technological change and, in particular, the migration of law enforcement agencies off the Wanganui computer.

11.1.5 Thirty one submissions were received on the discussion paper from a wide range of respondents, including local and central government and business amongst others.

11.1.6 Before turning to the detail of Part XI it will be helpful to canvass two matters to gain a full appreciation of the issues. First, I will say something about the Wanganui Computer Centre Act 1976 which was New Zealand’s first information privacy law. Then I will comment upon the nature of on-line access to personal information which is authorised by this part.

Wanganui Computer Centre Act 1976

11.1.7 This is not the place to offer a definitive history of, or guide to, the Wanganui Computer Centre Act 1976. Instead, some background information is provided here to set the discussion of Part XI in context. Perhaps at some stage the definitive history of privacy and freedom of information law in New Zealand will evaluate the importance of the 1976 law - whether it was a significant precursor to the Privacy Act and Official Information Act or simply a minor sideshow in the early years of major computerisation which distracted attention from the lack of privacy or open government legislation.¹

11.1.8 In 1971 an amendment to the Transport Act 1962 established a central register of all driver licences as a precursor to a central computer system. In 1972 the Government announced that it was to investigate a specially designed electronic data processing system for law enforcement agencies. Privacy concerns were already in consideration and it was stated that the proposed system:

“Would not be designed as a reference file on every New

¹ I am unaware of any published review of the Wanganui Computer Centre Act’s 15 year operation. Some information is to be found in the annual reports of the Wanganui Privacy Commissioner from 1977 through to 1993 and, concerning the Act’s first 6 years, in T J McBride, *Privacy Review*, 1984.

“When the Wanganui Computer Centre Act 1976 was introduced it provided for the first time an opportunity for the general public to examine information stored about them by a government agency and have it amended or corrected where necessary. In achieving this, the Act made a contribution in the field of human rights jurisprudence that has been justifiably claimed as being not only innovative but also unique. It broke new ground. It is of interest to note that when the OECD Guidelines were adopted several years later the principle of individual participation was included as being basic to any scheme for the legislative protection of privacy.”

- PL MOLINEAUX, REPORT

OF THE WANGANUI COMPUTER

CENTRE PRIVACY COMMISSIONER,

1985

Zealander. It would contain information already on record. It would not be an invasion of the privacy of the individual ... full safeguards to prevent unauthorised access or use of the information were being designed into the system.”²

11.1.9 During the 1972 general election the proposed law enforcement computer system was an issue and the Labour Party, then to become Government, distributed election literature entitled “Your Right to Privacy” warning of the risks. In 1974 the Labour Government announced that it intended to establish the law enforcement data system. In the closing session of that government’s term it introduced a Wanganui Computer Centre Bill and a Privacy Commissioner Bill as part of its plans to constrain the law enforcement computer centre and to provide privacy oversight. Although the Privacy Commissioner Bill did not survive a change of government, the new National Government did enact the Wanganui Computer Centre Act 1976. It conferred the privacy role proposed for the Privacy Commissioner upon a new Human Rights Commission.

11.1.10 The Wanganui Computer Centre Act established three new entities:

- *Wanganui Computer Privacy Commissioner* - an officer of Parliament;
- *Wanganui Computer Centre Policy Committee* - chaired by a Judge with a member of the NZ Law Society as Deputy Chairman, two members appointed by the Minister of State Services after consultation with the Attorney-General and interested groups, together with officials from the relevant departments;
- *Wanganui Computer Centre Management Committee* - made up of officials.

11.1.11 The Wanganui Computer Centre Act was described in its long title as:

“An Act to provide for the establishment and operation of a computer based information system to aid the Departments of Police and Justice and the Ministry of Transport to carry out effectively their roles in relation to the law and the administration of justice, and to ensure that the system makes no unwarranted intrusion upon the privacy of individuals.”

11.1.12 Much of the importance of the 1976 Act for privacy lay in the establishment of a Privacy Commissioner and the Policy Committee. The Wanganui Computer Centre Privacy Commissioner had a number of important functions such as to investigate complaints, carry out inquiries on the Commissioner’s own motion, and to give individuals access to information held about them on the system.³ The Policy Committee provided “civilian oversight” of the operation of the law enforcement database. It had amongst its functions the responsibility to:

“Determine the policy of the computer centre and the computer system relating to the privacy and the protection of the rights of the individual in so far as these are affected by the operation of the computer centre and the computer system ... ”⁴

11.1.13 Although the granting of access and correction rights, and the creation of the Privacy Commissioner and the Policy Committee, are the most important aspects of the Act from a privacy perspective I will say little more about them. In essence the Wanganui Computer Centre Privacy Commissioner’s complaints functions have been subsumed into the role of Privacy Commissioner while the

“The view is sometimes expressed that the Wanganui Computer Centre Act 1976 as it stands is cumbersome and too restrictive. Be that as it may any new appraisal will have to balance the needs of expediency against the requirement for privacy.”

- PL MOLINEAUX, REPORT OF THE
WANGANUI COMPUTER CENTRE
PRIVACY COMMISSIONER, 1985

² T J McBride, *Privacy Review*, page 29.

³ Wanganui Computer Centre Act 1976, sections 9 and 14.

⁴ Wanganui Computer Centre Act 1976, section 22.

rights of access and correction have been subsumed within the general rights provided in principles 6 and 7. The Wanganui Computer Centre Privacy Commissioner's function of operating a bureau to handle access requests has been discontinued. The role of a statutory Policy Committee has not been continued in any form. Some aspects of the Wanganui Management Committee, in a broader and non-statutory form, might be said to have been resurrected in recent years in the Justice Sector Information Committee.

- 11.1.14 There are other aspects of the Wanganui Computer Centre Act which have disappeared from our statute book. For example, specific legislation no longer exists to provide authorisation for this specific computer system. Indeed, in the latter years of the legislation it had become anomalous that while this major computer system had a specific legislated basis most other government computer systems did not.⁵ However, Part XI in a sense continues the Wanganui Computer Centre Act's function of *legitimising* the sharing of law enforcement information amongst several agencies through a common database - and in the future through the linking of separate databases. In this respect, Part XI essentially carried over aspects of sections 4 and 4A to 4E and the Schedule of the Wanganui Computer Centre Act 1976.
- 11.1.15 In considering Part XI of the Act in the light of this background and the legislative antecedents I have been mindful of:
- a background of concern amongst the New Zealand public in relation to large shared law enforcement databases;
 - the respect that has been accorded to those fears by legislators;
 - the work of the Wanganui Privacy Commissioner, as recounted in his annual reports;
 - the history of the Wanganui computer system, subject to strict controls, careful auditing, and rigorous oversight;
 - the fact that while the Privacy Act continues many of the key features of the Wanganui Act in a general framework there are nonetheless significant safeguards that have disappeared.⁶

On-line access

- 11.1.16 The Privacy Act, unlike some earlier forms of data protection laws such as the Wanganui Computer Centre Act, seeks to be “technology neutral” “media neutral” and “sector neutral”. Indeed, it is sometimes referred to as third or fourth generation privacy law with its application to “information” held in the public and private sectors, with earlier generation laws covering just automatically processed data, information contained in documents or information solely held in the public sector.
- 11.1.17 Notwithstanding its general technology neutral approach the Act does directly address certain information privacy issues in terms of certain computer applications. For example, public register privacy principle 3 constrains electronic transmission of personal information from a public register and information matching rule 3 prohibits the use of on-line computer connections in authorised information matching programmes.
- 11.1.18 Unlike those other two provisions, Part XI makes no mention of any computer database or computer technology. Nonetheless, it does seem relatively plain from the legislative history that it is directed to the type of arrangements main-

⁵ One that did was the Health computer system operated under the former section 22B of the Health Act 1956. Similar controls existed in section 62A of the Hospitals Act and section 51 of the Area Health Boards Act. The 3 sections were enacted in 1988 to allay privacy concerns over the privatisation of the health computer system and repealed in 1993 with the enactment of the Privacy Act.

⁶ For example, while the right of access has been successfully subsumed into principle 6, there is no longer a policy committee, an offence of coercing access requests, or independent oversight of the placing of remote terminals.

tained under the Wanganui Computer Centre Act 1976. In particular, the provisions of Part XI, and the Fifth Schedule, are directed towards providing authorisation for, and limits upon, the on-line accessing of law enforcement databases by other law enforcement agencies. That this is not entirely plain from the words of Part XI might be asserted as a criticism of the Part, but that is the basis upon which I have understood the provisions as have the law enforcement officials who have dealt with it.

- 11.1.19 However, the Part and the associated schedule, need not be read as simply continuing the “Wanganui” arrangements. The Wanganui Computer involved a shared database maintained in a single location to which law relevant enforcement agencies have access. The categories of information stored on the database were assigned as the responsibility of a particular agency, now known as the holder agency. The other agencies entitled to have access to that information are now identified as accessing agencies.
- 11.1.20 However, all law enforcement agencies will have migrated off the Wanganui Computer before the end of 1999.⁷ The Part XI and Fifth Schedule arrangements are intended to continue whereby the holder agencies will continue to separately hold the respective information, no longer in a shared database but in their own systems. The accessing agencies will continue to have on-line access to the information in much the same way (in legal, if not technical, terms).
- 11.1.21 There is something different in quality in these on-line access arrangements compared with the normal information handling and processing encountered by the vast majority of agencies. Most agencies hold some personal information and they will, on occasion, share that with other agencies. This might be initiated by the agency holding the information which may disclose that information elsewhere. Or perhaps another agency will request the information from the agency holding it and it will be released in response to that. In other cases the individual concerned will become involved and request the information directly or ask that it be transferred to a third party. The information privacy principles handle each of these arrangements perfectly well. To make the disclosure the agency that holds the information must “believe on reasonable grounds” that one of the exceptions to information privacy principle 11 applies.
- 11.1.22 However, in the on-line access arrangements contemplated by Part XI, and formerly by the Wanganui Computer Centre Act, the nature of the arrangement is somewhat different. The agency that actually holds the information makes no judgment in relation to the release of the information on a case by case basis. Instead, a blanket approval is given to another agency to have access to holdings of information. There are very few other agencies that have such arrangements. It is almost like a department or business giving another department or business the keys to its front door and filing cabinets together with an index to its files. Few agencies are willing to run that risk with sensitive data but in the law enforcement sector, subject to controls, it is essential.
- 11.1.23 The nature of on-line access brings with it a need to impose certain restraints and take certain safeguards. Part XI spells some of these out. For example, law enforcement agencies are not authorised to share information with just anybody, only the agencies specified. Other agencies may, on occasion, have need of the information and this will be shared on a need to know basis consistent with the information privacy principles and other legislation. Furthermore, the law enforcement agencies do not give each other complete access to their

“The current schedule makes for efficient administration for the agencies involved by not requiring each request to be authorised and provides for openness of the sharing arrangement by having a schedule and an approval process.”

- WELLINGTON CITY COUNCIL,
SUBMISSION H6

⁷ With at least one benefit being mitigation of Y2K problems. See Report of the Government Administration Committee, *The Y2K Inquiry: Inquiry into the Year 2000 Date Coding Problem*, April 1998, pages 88 and 99.

entire information holdings. The information is segmented and authorisation to have access to parts of the database is provided, again, on a need to know basis. For example, the detail of “victim identity” in the Police information holdings is available solely to the Department for Courts. Furthermore, this entry and others are subject to express limits. In that case, the Department for Courts’ access is limited to identity details for the purpose of providing assistance to victims in accordance with the Criminal Justice Act and the Victims of Offences Act.

- 11.1.24 The nature of on-line access is such that it would be difficult to operate the information sharing arrangements that exist in the law enforcement sector without an authorisation of the type provided in the Fifth Schedule. Without this statutory authorisation, sharing arrangements would be open to challenge for being in breach of, say, information privacy principles 2 or 11. Accordingly, the Part has a *legitimising* or *authorising* function. However, through the limits placed on access in the Fifth Schedule, the Part has a *constraining* or *controlling* function. The resultant Schedule provides a degree of transparency as to the on-line information sharing arrangements between the named law enforcement agencies.

SECTION BY SECTION DISCUSSION

11.2 SECTION 110 - Interpretation

- 11.2.1 Section 110 defines four terms used in Part XI.

Accessing and holder agencies

- 11.2.2 The definitions of “accessing agency” and “holder agency” are limited to any “public sector agency” (a term which is itself defined in section 2) for the time being specified in the Fifth Schedule as, respectively:

- an agency to which law enforcement information held by a holder agency is available;
- an agency the records of which are available to an accessing agency.

Neither definition was included in the Wanganui Computer Centre Act although the use of a schedule to identify the agencies which respectively hold and access any particular information is carried forward from that Act.⁸

Law enforcement information

- 11.2.3 The definition of law “enforcement” information is essentially the same as appeared in the Wanganui Computer Centre Act (the differences simply being the change in schedule numbering and the use of “individual” rather than “person”).

Local authority

- 11.2.4 The definition of “local authority” is taken from section 4E(2) of the Wanganui Computer Centre Act 1976.⁹ The origin of this definition in the 1976 Act provides the explanation for the fact that this definition of “local authority” differs from the definition set out in section 2. The section 2 definition is derived from the Local Government Official Information and Meetings Act 1987. It is not ideal for an Act to have two definitions of the same term since this theoretically may create confusion. In fact, no difficulties have been encountered because, as I explain at paragraph 11.4 in relation to section 112, local authorities have not utilised Part XI to obtain access to law enforcement information.

- 11.2.5 In recommendation 139 I propose that section 112 be repealed. If this is accepted the definition of “local authority” could also be repealed.

⁸ The Wanganui Computer Centre Act 1976, section 2, contained a definition of “user departments” which brought together what now would be known as accessing and holder agencies.

⁹ As inserted by a 1989 amendment.

11.3 SECTION 111 - Access by accessing agencies to law enforcement information

11.3.1 Section 111 provides that:

“An accessing agency may have access to law enforcement information held by a holder agency if such access is authorised by the provisions of the Fifth Schedule to this Act.”

11.3.2 This section is the key operative provision in Part XI. It is the provision which legitimises information sharing amongst the relevant law enforcement agencies as provided for in the Fifth Schedule. It is, in the words of section 7 of the Act, a “provision that is contained in [an] enactment and that authorises or requires personal information to be made available”.

11.3.3 No definition is included of the term “access”. The Wanganui Computer Centre Act defined the term as follows:

“Access’, in relation to the computer system, means the placing of information on that system and the retrieval of information from that system.”¹⁰

11.3.4 Notwithstanding the lineage of Part XI directly from the Wanganui Computer Centre Act, I do not believe that such a meaning is intended in this context. Instead, I think what is meant is something like the second meaning ascribed to “access” in the *Concise Oxford Dictionary*, that is “the right or opportunity to reach or use or visit; admittance (has access to secret files; was granted access to the prisoner).” The Wanganui Computer Centre Act definition included within it the placing of information on the computer system. Part XI has not attempted to provide the authority for such matters.¹¹ Instead, the approach of the Part seems to be directed towards authorising access to information but not dealing with (whether by way of authorisation, prohibition or regulation) other matters concerning the use, modification or safeguarding, of information which were matters dealt with by the former Wanganui Computer Centre Act. The intention was, I believe, that those other matters be addressed by the normal application of the information privacy principles and any other relevant legislation.

11.3.5 Since Part XI, unlike the Wanganui Computer Centre Act, does not attempt to regulate all handling and processing of the information identified in the Fifth Schedule there are questions as to what the appropriate role of the Part is or should be. Questions to promote discussion of these issues were included in the discussion paper. One school of thought would favour diminishing the application and relevance of Part XI particularly as agencies move off the Wanganui computer system and the 1976 set up is no longer recognisable. That approach might see these matters dealt with by application of the information privacy principles coupled with any applicable specific legislation and, as necessary, protocols or contracts between the agencies sharing information. The other school would seek to enhance the role of Part XI by bringing within it other public sector agencies having law enforcement functions where those agencies share information. Further enhancement might involve, for example, prohibiting agencies to which the Schedule applies from sharing information *otherwise* than in accordance with the provisions of the Fifth Schedule.¹²

¹⁰ Wanganui Computer Centre Act 1976, section 2.

¹¹ However, access is made available in some entries in the Fifth Schedule in a manner which is limited to cases where an agency has business to add information to a particular record - see entry relating to Department for Courts access to particulars of the identity of persons who have been charged with an offence.

¹² An example would be to prohibit a local authority from obtaining details of the motor vehicle and driver licence registers otherwise than in accordance with a *Gazette* notice that had been issued under section 113 in respect of that agency.

“The issue can be seen as being, not the number of agencies collecting, using, or accessing the same personal information, but rather the extent to which the various privacy principles are reflected in the information management practices applied to the databases. The Group favours a principled and flexible approach as opposed to a prescriptive approach. Part XI of the Act and the Fifth Schedule should be repealed.”

- NZ LAW SOCIETY PRIVACY WORKING GROUP, SUBMISSION H15

11.3.6 I do not see the scope of Part XI as set in stone and a case could be made to bring further law enforcement agencies into the scheme as accessing or holder agencies. My review has not uncovered a need for that yet. I have concluded that Part XI fulfils a valuable function given the nature of the on-line access of information that is central to law enforcement and justice arrangements in the late 1990s. The Schedule provides a degree of transparency.

11.4 SECTION 112 - Local authorities may be authorised to have access to law enforcement information

11.4.1 The Minister of Justice may, by notice in the *Gazette*, authorise a local authority to have access to certain limited law enforcement information provided for in the Fifth Schedule to the Act. Such authority may be granted on condition and can be amended or revoked. Section 112 also continues the effect of notices given under the Wanganui Computer Centre Act.

11.4.2 I have examined two main issues in relation to this provision:

- whether there continues to be any need for local authorities to have such access;
- whether notices given under the Wanganui Computer Centre Act should continue in force.

Current local authority access

11.4.3 The only law enforcement information to which a local authority can currently access pursuant to a *Gazette* notice, is:

- the national register of motor vehicles maintained by the Ministry of Transport; and
- the national register of drivers' licences maintained by the LTSA.¹³

Since no local authority has sought, or been granted, a notice under section 112 the only local authorities authorised to have such access are those in respect of which a notice was given under the Wanganui Computer Centre Act 1976 which remained in force immediately before the commencement of the Act.

11.4.4 Four *Gazette* notices were issued pursuant to section 4E of the Wanganui Computer Centre Act. These related to six local authorities, none of which has actually utilised its access rights.¹⁴ The reasons for the lack of interest on the part of local authorities, to access the law enforcement information are readily apparent. Since section 4E was first enacted in 1980 there have been significant changes in respect of local authority functions in relation to driver licensing (which is now handled nationally rather than at local body level). None of the local authorities which maintained traffic enforcement departments in 1980 continue to do so. Enhancements have also been made in relation to the availability of the motor vehicle register to public register provisions.

11.4.5 The explanation from the Hutt City Council is typical of the replies received in response to enquiries about the continuing use of the entitlements under the *Gazette* notices. The Hutt City letter stated:

“The Council was originally given approval to access the drivers licence register and the motor vehicles register because it acted as a driver licensing agency for the Ministry of Transport. Such a function is not core Council business and Council no longer provides this service. Council has never exercised its rights to access information for the driver licence register or motor vehicles register of the Wanganui Computer and does not anticipate that it would need to exercise these rights to carry out its parking control functions.

¹³ See Privacy Act, Fifth Schedule.

¹⁴ Confirmed in correspondence with various councils and EDS (New Zealand) Ltd.

“Information from the motor vehicles register is crucial to Council’s core service of parking control. However, Council obtains the information it requires from the Land Transport Safety Authority’s motor vehicle register in Palmerston North.

“It is the understanding of Council officers that to access the ‘Wanganui Computer’ Council would require a separate secure PC link (remote terminal). Council does not have such a link and does not anticipate that it would ever require such a link to carry out Council’s current powers with respect to parking controls.”¹⁵

Need for local authority access

- 11.4.6 It seems plain that local authority access to law enforcement information pursuant to section 112 is currently unnecessary. In particular:
- since provision was made in 1980 only six local authorities have obtained such approval;
 - of those six, none ever installed a remote terminal or utilised the permitted access;
 - no local authorities have sought, or obtained, notices under section 112 in the years since the enactment of the Privacy Act.
- 11.4.7 My view is that if such access is not needed the provision should probably be deleted from the Act. Accordingly, my prime recommendation is that section 112 be repealed. Consequently the definition of “local authority” in section 110, and the references to local authorities in the Fifth Schedule, could also be repealed.



RECOMMENDATION 139

Section 112 providing for local authorities to be authorised to have access to law enforcement information should be repealed together with the definition of “local authority” in section 110 and the references to local authorities in the Fifth Schedule.

Amendments if local authority access retained

- 11.4.8 It may be that further examination by the Ministry of Justice will suggest that provision for local authorities to have access should be retained in case it is necessary in the future. In my view, any access that cannot presently be forecast should not be provided for in this way but instead should come before Parliament as an amendment to the Privacy Act in due course. However, if, unknown to me, there is a good case in the medium term for local authorities to have access to law enforcement information through these provisions then certain amendments should nonetheless be made.
- 11.4.9 First, while local authorities have continuing need to have access to the motor vehicles register (albeit that they currently find it more convenient to simply deal with the Motor Vehicle Registration Centre in Palmerston North), there appears to be no continuing need for access to the driver licence register.
- 11.4.10 Second, there are unacceptable privacy risks in continuing the notices given under the Wanganui Computer Centre Act. The notices given in 1990, 1992 and 1993, were based on a set of assumptions concerning the need for access which is not supported by current conditions. Section 112(4) should be repealed so that the *Gazette* notices given under the Wanganui Computer Centre Act cease to have any legal effect.

“Care is needed to ensure that agencies are only included in the Fifth Schedule where both the importance of their function and the frequency of their requests makes this necessary. We note that there is increasing demand from agencies with some law enforcement functions to share information with law enforcement agencies. This is becoming technically feasible as agencies exit from the Law Enforcement System on the Wanganui Computer, although the Fifth Schedule may not prove to be the appropriate mechanism to address this issue.”

- MINISTRY OF JUSTICE, SUBMISSION H14

¹⁵ Submission H11.

**RECOMMENDATION 140**

If section 112 is not repealed in its entirety then the reference to local authorities in the Fifth Schedule relating to the national register of drivers' licences should be repealed.

- 11.4.11 The existing *Gazette* notices issued under section 4E of the Wanganui Computer Centre Act, none of which are being utilised, should be revoked if there is no present prospect of them being utilised. If any of the six affected local authorities wish to continue to retain such authority a process should be instituted to prepare a new *Gazette* notice to be issued under section 112 which would replace and enable the revocation of the earlier notice. When that process has been completed then subsection (4) of section 112 should itself be repealed.
- 11.4.12 Conditions on the notices given under the Wanganui Computer Centre Act are no longer satisfactory. The *Gazette* notice of 17 July 1990 has six conditions. The three subsequent notices each refer to that notice and incorporate the relevant conditions.¹⁶ Conditions(c), (d), and (f) each rely upon directions, approvals, inspections, and audit, by a body which no longer exists - the Wanganui Computer Centre Policy Committee. The issue of a new *Gazette* notice would give an opportunity to reconsider the appropriate conditions.

**RECOMMENDATION 141**

All existing approvals given under section 4E of the Wanganui Computer Centre Act 1976 should be reviewed and:

- (a) any that are unnecessary should be revoked;**
(b) any which need to be continued should be replaced, within a reasonable time, with a new notice carrying appropriate conditions issued under section 112.

11.5 SECTION 113 - Amendment to Fifth Schedule

- 11.5.1 By operation of the “sunset” clause in section 114, section 113 has now expired. Presently the Fifth Schedule may be amended by further Act of Parliament. However, during the Act’s first four years of operation the Schedule was, through reliance upon section 113, able to be amended by Order in Council.¹⁷
- 11.5.2 As already noted the Fifth Schedule of the Privacy Act was, in essence, previously contained in the Schedule to the Wanganui Computer Centre Act 1976. There was a procedure for supplementing the provisions of the Schedule to the 1976 Act by Order in Council.¹⁸ The Privacy of Information Bill (which became the Privacy Act) provided for amendment to the Schedule to be made by Order in Council. However, when the bill was considered by the Select Committee after its introduction, that committee decided that amendments to the Fifth Schedule were more appropriately the province of Parliament than the Executive. Parliament accepted the Select Committee’s advice and allowed a period of three years for further work to be undertaken on identifying existing uses of law enforcement information and for any implementing amendments to be made during that period by Order in Council.
- 11.5.3 Thus, at the time that the Privacy Act was passed, section 113 provided that the Fifth Schedule could be amended by Order in Council made on the advice of the Minister of Justice given after consultation with the Privacy Commissioner. However, this ability to amend the Fifth Schedule by way of Order in Council was to expire on 1 July 1996. The progress anticipated on researching the

¹⁶ See *Gazette* notices of 28 September 1990, 11 November 1992 and 20 April 1993.

¹⁷ Originally amendment by Order in Council was allowed for three years during an implementation phase. This was extended for 12 months by the Privacy Amendment Act 1996.

¹⁸ Wanganui Computer Centre Act 1976, section 30.



“It is important that the law is seen to be upheld and that there are no hidden or secret agreements between law enforcement agencies. By publishing the schedule this retains the transparency and would provide an assurance to the public that there is some control over the use of the information.”

- CLIVE COMRIE, SUBMISSION H1

“Amendment to the Fifth Schedule should, for purposes of transparency, continue, as at present, to be by Act of Parliament.”

- NZ EMPLOYERS FEDERATION,
SUBMISSION H5

existing uses of information, and the consequent making of any necessary amendments, was not rapid and the work was not completed within 3 years. This was partly due to the various restructurings which were being planned, or implemented, during the early to mid 1990s.¹⁹ These restructurings themselves required work to be done to reflect information sharing in the Fifth Schedule. Accordingly, a case was made for an amendment to sections 113 and 114 allowing the Order in Council amendment procedure to continue for a further 12 months. I supported the amendment on the basis that reorganisation had made completion of the task within 3 years more difficult than anticipated but that it was nonetheless important that the task be undertaken.

- 11.5.4 Justice sector agencies would like to have a procedure to amend the Fifth Schedule without the need to obtain an amending Act of Parliament.²⁰ They would tend to make their case based upon the desire for flexibility, and the desirability of a reasonably rapid response, to changing technology and issues arising from the exit from the Wanganui Computer system. While all businesses and departments are familiar with the traumas and uncertainties surrounding the move to new computer systems, few will have faced that prospect having worked with a shared mainframe computer system, such as Wanganui, for over two decades.
- 11.5.5 The importance of information management in this sector, the significant changes, and the present degree of uncertainty, persuades me that there is a case for resurrecting a less restrictive amendment process than Act of Parliament for changing the Fifth Schedule. However, I am suspicious of the surveillance potential of overly “flexible” arrangements for sharing information amongst the law enforcement arms of the state. I am also mindful of the Select Committee’s firm views, affirmed in 1993 and 1996, that the Order in Council process should be available for only a limited time, after which such decisions should revert to Parliamentary control.
- 11.5.6 Accordingly, while I support the revival of a process for amendment by Order in Council my recommendation takes account of the Select Committee’s misgivings. My proposal is that the Order in Council amendment processes be revived only for a limited period to take account of the uncertainties faced by the sector during the period of migration off the Wanganui Computer system and in establishing and implementing separate databases. I consider that five years should be adequate.²¹
- 11.5.7 The requirement is quite straightforward and picks up upon the Select Committee’s earlier insistence on a limited three year period later extended to four years. It is to be preferred over the alternative that I considered, which was to transfer the entire Fifth Schedule into regulations.²²



RECOMMENDATION 142

Provision should be made to allow the Fifth Schedule to be amended by Order in Council subject to a five year sunset clause.

¹⁹ In a sector which had been almost untouched by structural change since at least the time of Wanganui Computer Centre Act 1976, there was during these years, an amalgamation of the Police and Ministry of Transport, the creation of the Land Transport Safety Authority, the division of the Department of Justice into a Ministry and two departments, and various reallocation of responsibilities amongst new and existing entities.

²⁰ See, for example, submissions H1, H14, S33 and S58.

²¹ A five year period will also allow the matter to be re-examined at the next periodic review under section 26.

²² The advantages of moving the Schedule into regulations include the end of section 113 as a “Henry VIII clause”. Such clauses, which allow primary legislation to be amended by secondary legislation, are not favoured for constitutional reasons. The transfer to regulations would also lead to a slightly “streamlined” Act for regular users not concerned with technical law enforcement information issues. However, the alternative recommended is considered to offer greater transparency and reassurance, be easier from a drafting perspective and continue familiar arrangements.

“It is inefficient to have to go to Parliament each time a technology change or law enforcement requires an amendment to the Act. Regulation making powers, or changes by ministerial notice make changes simpler and they remain subject to the scrutiny of the Regulations Review Committee of Parliament. That said, the Act provides certainty and a level of control over sensitive information and a higher level of transparency because it goes through Parliamentary debate and Select Committee process.”

- DEPARTMENT FOR COURTS,
SUBMISSION S33

11.6 SECTION 114 - Expiry of power to amend Fifth Schedule by Order in Council

- 11.6.1 Section 114 expired on 1 July 1997. The issues surrounding this expiry have been discussed in relation to the previous section. If the process for amending the Fifth Schedule by Order in Council is revived section 114, or something similar to it, will need to be enacted.

“If it was not deemed appropriate to require the full legislative process to be embarked upon for a change to the schedule then, as a matter of policy and administration, a wider consultative exercise than that adopted when amendment by Order in Council is prescribed would be favoured.”

- NZ LAW SOCIETY PRIVACY

WORKING GROUP, SUBMISSION

H15

Part XII

XII

Miscellaneous Provisions

349

“I have no doubt that the intention of the Wanganui Computer Centre Act was simply to enable the public to check for themselves whether the official record was correct as far as they were concerned. It exceeds the legislative purpose if pressure is brought to bear on members of the public to supply information from the database that is and always was intended to be confidential as far as possible.”

- P L Molineaux, *Report of the Wanganui Computer Centre Privacy Commissioner*, 1987

“You questioned whether it is appropriate to create an offence of misleading an agency in order to gain access to information, either by impersonating the individual concerned or misrepresenting that they have an authorisation from that person. You also suggested that there might be an offence of knowingly destroying information to which a person is entitled in order to deny the person access to it. In both of these instances you note the Privacy Act obliges agencies to open their files to individuals where previously they may have kept them far more securely closed to outsiders, and that the agency and the individual are at risk. It would not be inappropriate to incorporate an offence provision in these circumstances. Obviously an eye would need to be kept on whether it is appropriate to invoke the sanctions of the criminal law in what is essentially a civil context. In our view the examples you give are appropriate ones”.

- Crown Law Office, submission G16

“The issue of computer crimes is one that needs to be addressed with some urgency. The Group does not, however, consider that the Privacy Act is the appropriate vehicle for addressing the issue.”

- NZ Law Society Privacy Working Group, submission G22

12.1 INTRODUCTION

12.1.1 Part XII brings together a series of unrelated provisions.

12.1.2 The provisions are grouped into six categories:

- general - sections 115 to 120;
- delegations - sections 121 to 125;
- liability and offences - sections 126 and 127;
- regulations - section 128;
- amendments, repeals and revocations - section 129;
- transition provisions and savings - 130 to 133.

SECTION BY SECTION DISCUSSION

12.2 SECTION 115 - Protection against certain actions

12.2.1 Section 115 protects requesters and providers of personal information, as well as others, from legal liability arising from the mere use of, or compliance with, the Act. These immunities are limited to actions taken in good faith pursuant to information privacy principle 6. The section is derived from section 48 of the Official Information Act 1982, as inserted in 1987. The drafting of the original section 48 of the Official Information Act was deficient and the 1987 provision was intended to remedy those deficiencies.¹ However, commentators on the Official Information Act have suggested that there remains a drafting deficiency with section 48 - and hence section 115 of the Act.

12.2.2 The issues have been described by Dr Paul Roth in *Privacy Law and Practice* as follows:

“A comparison of subs(1)(a) and (b) with subs(2), might suggest that there is some significance to the distinction drawn between ‘the making available of [personal] information’ on the one hand, and ‘the making available of, or the giving of access to, any personal information’ on the other. A similar distinction is drawn in both s.48 of the OI Act and s.41 of the LGOIM Act. Elsewhere in the OI Act a distinction is indeed maintained in relation to information to which there is a right of process (Part II, dealing with official information in the general sense) which is made available, and information to which there is a right of access (Part III and IV, dealing with certain forms of official information and personal information) to which access is given. However, it is unlikely that this subtle distinction would have any significance in regard to the immunities conferred by the relevant legislation. Accordingly, the distinction in s.48 of the OI Act (and carried over into subsequent freedom of information legislation) has been suggested to be an oversight in drafting: see I Eagles, M Taggart, G Liddell *Freedom of Information* (Auckland, 1992), p 614.”²

12.2.3 Dr Roth notes that this particular issue was expressly considered by the Select Committee which studied the Privacy of Information Bill. He states:

“The distinction was noted in the report of the Department of Justice to the Privacy of Information Sub-Committee of the Justice and Law Reform Committee (22 January 1993, p30), which commented that explicit limitations of the section to principle 6 would make it clear that the section was based on, and thus should have the same construction as, s.48 of the OI Act.”³

12.2.4 Given that the select committee had the issue drawn to its attention, took advice and made an informed decision about the drafting, the matter could be left there. Indeed, I am unaware that the issue has caused any difficulties. However, it must be borne in mind that the select committee had before it only the privacy legislation. It could not, of course, have amended the Official Information Act. Therefore, if the Privacy of Information Bill had struck out in a new

¹ Section 48, and its original deficiencies, are discussed in *Freedom of Information in New Zealand*, pages 613-614.

² *Privacy Law & Practice*, paragraph 1115.4.

³ *Privacy Law & Practice*, paragraph 1115.4.

direction it would quite possibly have caused new difficulties of interpretation and consistency. However, we are now at a point whereby further consideration could be given to this issue so that, if appropriate, a consistent amendment could be made to each of the Privacy Act, Official Information Act, and Local Government Official Information and Meetings Act.



RECOMMENDATION 143

Consideration should be given to the merits of making consistent amendments to:

(a) section 115 of the Act;

(b) section 48 of the Official Information Act 1982; and

(c) section 41 of the Local Government Official Information and Meetings Act 1987;

to meet the perceived difficulties of interpretation raised by the distinction in the first and second subsections of each of these provisions between “the making available of information” and the “making available of, or the giving of access to, information”.

12.3 SECTION 116 - Commissioner and staff to maintain secrecy

12.3.1 This section requires:

- the Commissioner; and
- every person engaged or employed in connection with the work of the Commissioner;

to maintain secrecy in respect of all matters that come to those persons’ knowledge in the exercise of their functions under the Act. However, as Commissioner, I may disclose such matters as in my opinion ought to be disclosed for the purposes of giving effect to the Act - but this does not extend to information that might prejudice certain listed public interests such as national security and cabinet confidences.

12.3.2 The provision is necessary since a variety of material which must remain secret is brought into my office pursuant to a variety of my functions, especially my investigative functions.⁴ For example, I may at any time be holding thousands of copy documents which are being reviewed to see whether the agencies that hold them should release the material to requesters. I am subject to both the Official Information Act and the rights of access conferred by information privacy principle 6, but it would undermine the review process if such documentation could be sought directly from me. The secrecy obligation goes beyond the circumstances where I might receive a request or demand for information and also constrains my own disclosure of certain sensitive information.

12.3.3 Naturally a secrecy obligation of the type imposed by section 116 needs, to be effective, to also apply to former staff, consultants and commissioners, after they leave the office. I expect that this section, and section 96 to which it is linked, may be open to be construed so as to apply to former staff. However, it does not say so explicitly. By contrast the Serious Fraud Office Act 1990, which has a secrecy provision similar to section 116 (section 36), also has a section imposing a continuing obligation in respect of persons ceasing to be members of the Serious Fraud Office (section 44).

12.3.4 The Australian Privacy Act’s secrecy provision applies to:

“a person who is, or has at any time been, the Commissioner or a member of staff or is acting, or has at any time acted, on behalf of the Commissioner.”⁵

12.3.5 It would seem desirable to make the position explicit. To avoid cluttering the Act with a new section modelled upon section 44 of the Serious Fraud Office

⁴ Privacy Act, section 90(1), makes clear that every investigation is to be carried out in private.

⁵ Privacy Act 1988 (Australia), section 96(1).

Act, I suggest that section 96(1) be amended or that a new provision appear in the First Schedule.



RECOMMENDATION 144

Section 96, or the First Schedule, should be amended so that the obligation of secrecy clearly extends to former Commissioners and persons formerly engaged or employed in connection with the work of the Commissioner.

12.4 SECTION 117 - Consultation with Ombudsmen

12.4.1 One of the consequences of having a secrecy provision like section 116, is that it becomes desirable for further provisions to outline the circumstances in which otherwise secret information can be disclosed. Section 117 is such a provision which provides the authority for sharing information with an Ombudsman during consultations. However, the secrecy provision is only one reason for having consultation provisions. They are also intended to foster co-operation and avoidance of duplication of work. The Ombudsmen, and their office, are an important part of the fabric of the public sector in New Zealand. I have valued the discussions that I have had with the present and former Ombudsmen.

12.4.2 The first type of consultation anticipated in paragraph (a) involves the making of a determination under section 72 - that is, the referral of a complaint to an Ombudsman where that complaint more properly comes within the jurisdiction of the Ombudsmen. Under paragraph (b) I may consult in relation to any matter arising in the course of an investigation under Part VIII of the Act. Such consultations are particularly valuable where there is:

- in the subject matter of the complaint, an inter-relationship between the Privacy Act and the official information legislation;
- an investigation also being undertaken by the Ombudsmen under the official information legislation or the Ombudsmen Act, or it might be desirable for there to be such an investigation.

12.4.3 Paragraph (c) anticipates consultation on matters relating to privacy whether or not a complaint has been lodged. Although not as frequent as the other consultations, these do occur from time to time as it is desirable for the Commissioner and Ombudsmen to be aware of each other's views on such matters. A recent example would be some general consultations, which have flowed from, but are not directly related to, the privacy and administrative issues arising in relation to adoption information and the interests of adopted persons, birth mothers, adoptive parents and the descendants and siblings of the various parties.

12.4.4 The other consultations held with the Ombudsmen arise pursuant to sections 29B of the Official Information Act 1982 and section 29A of the Local Government Official Information and Meetings Act 1987. These oblige the Ombudsmen to consult with the Privacy Commissioner when reviewing a decision to withhold information on a complaint under that legislation before forming a final opinion in relation to the merits of refusing a request on grounds related to privacy. I have considered these consultations to be of particular importance amongst the functions I carry out arising in relation to other enactments. I have seen it as important to be personally involved in each such consultation although this involves a not inconsiderable commitment of time and resource.

12.4.5 The following table gives the number of formal consultations with the Ombudsmen under the official information statutes recorded since 1993:

FIGURE 4. OMBUDSMEN CONSULTATIONS				
1993/94	1994/95	1995/96	1996/97	1997/98
22	26	60	87	77



12.5 SECTION 117A - Consultation with Health and Disability Commissioner

12.5.1 Section 117A was inserted by section 81(2) of the Health and Disability Commissioner Act 1994 with effect from 20 October 1994. There have been fewer formal consultations with the Health and Disability Commissioner compared with those undertaken with the Ombudsmen. The provision is not in need of amendment.

12.6 SECTION 117B - Consultation with Inspector-General of Intelligence and Security

12.6.1 Section 117B providing for consultation with the Inspector-General of Intelligence and Security was inserted in 1996. I supported the inclusion of the provision in my report on the Intelligence and Security Agencies Bill.⁶ As with the other consultation provisions, the section marks out the point of interaction between our respective functions, encourages consultation in matters affecting both offices, and provides authority for necessary disclosure of confidential information in the course of those consultations.

12.6.2 I have concluded that it would be desirable to create a single generic consultation provision which would combine sections 117, 117A and 117B and provide a framework for the addition of any further statutory bodies which require to be listed. It may even be desirable to remove the detail of the types of consultations to a new schedule. This would have two columns. The first would indicate the officer with whom the Commissioner would undertake consultation with the second modelled upon items (a) to (c) of sections 117, 117A and 117B.



RECOMMENDATION 145

Sections 117, 117A and 117B should be combined into a single consultation section with consideration given to placing the details of the officer with whom consultation is to be undertaken and the purposes of such consultation in a new schedule.

12.6.3 I have considered the merits of including consultation provisions with other statutory bodies. One such statutory body, subject to a secrecy provision, which would seem to be an appropriate candidate is the Police Complaints Authority.⁷ Others would include the Human Rights Commission and Broadcasting Standards Authority.



RECOMMENDATION 146

Consideration should be given to making provision, along the lines of sections 117 to 117B, for consultation with other statutory bodies such as the Police Complaints Authority.

12.7 SECTION 118 - Corrupt use of official information

12.7.1 Under section 118:

- the Privacy Commissioner; and
- every person engaged or employed in connection with the work of the Commissioner;

are deemed to be “officials” for the purposes of sections 105 and 105A of the Crimes Act 1951 which provides for the prosecution for the corrupt use of official information or the use of personal information disclosed corruptly. This

⁶ Report by the Privacy Commissioner to the Minister of Justice on the Intelligence and Security Agencies Bill, 26 February 1996.

⁷ The relevant secrecy provision is Police Complaints Authority Act 1988, section 32.

is a standard provision in legislation which creates new public entities to ensure that the bribery and corruption laws effectively extend to the new bodies.

- 12.7.2 Section 105B of the Crimes Act 1961 exists to make unlawful the trade in corruptly disclosed personal information. Section 105B was, on my suggestion, inserted into the Crimes Act in 1993 on the recommendation of the committee which studied the Privacy of Information Bill.
- 12.7.3 I supported the enactment of section 105B which implemented a recommendation of the New South Wales Independent Commission against Corruption (ICAC) which had just completed a major study into the trade in corruptly disclosed government information.⁸ What was uncovered by ICAC in New South Wales was a disturbing trade in which officials were being paid to release government information - usually to private investigators. In many cases the private investigators were procuring the information for reputable organisations, like banks and insurance companies, which sometimes even directed which Government database was likely to hold the information sought. Existing law in New Zealand, and no doubt New South Wales, was effective to criminalise the actions of the officials who corruptly disclosed the information, and the private investigators who bribed those officials. However, the trade continued to flourish because a market existed. Section 105B is intended to make it clear that anyone who knowingly uses such corruptly obtained information will themselves commit an offence.
- 12.7.4 When the opportunity arose in 1994, I recommended that amendments be made to the Private Investigators and Security Guards Act 1975 so that a person who has been convicted of an offence under section 105B should be barred from being licensed as a private investigator.⁹ I made this recommendation on the basis that ICAC evidence showed that private investigators were, in nearly all cases, the “middle men” who procured the corrupt release of official information and enabled the trade to flourish. I am pleased to say that reference to section 105B was made.¹⁰

12.8 SECTION 119 - Exclusion of public interest immunity

- 12.8.1 Section 119 prevents claims of public interest immunity, in order to exclude evidence, from arising in investigations by the Privacy Commissioner, proceedings before the Complaints Review Tribunal, or in judicial review proceedings. However, this exclusion does not give anyone an additional right to obtain information that they would otherwise not have.
- 12.8.2 The provision is derived from section 11 of the Official Information Act 1982. In discussion of that provision it is noted in *Freedom of Information in New Zealand* that:

“The Act strengthens the courts’ hand in reviewing decisions under the OIA by excluding claims of public interest immunity. However, the draftsperson was obviously concerned that an unsuccessful complainant before the Ombudsman might take advantage of this and initiate review proceedings as an indirect means of obtaining information which is protected by the Act. To prevent this occurring the following words were added to section 11(1): ‘but not

⁸ Independent Commission against Corruption, *Report on Unauthorised Release of Government Information* (3 volumes), August 1992.

⁹ See Report of the Privacy Commissioner to the Minister of Justice on the Law Reform (Miscellaneous Provisions) (No 3) Bill, October 1994.

¹⁰ See Private Investigators and Security Guards Act 1975, section 17.

so as to give any party any information that he would not, apart from this section, be entitled to’.

“Taken as a whole, section 11 seems to envisage that the court will examine the withheld material *in camera* with a view to acting on it as evidence even though it will be kept from the requesting party during the proceedings. While, generally speaking, it is undesirable and almost certainly unlawful for a court to rely on evidence that one side has not seen, this practice appears to be sanctioned by section 11(1) and is necessary to ensure that all the relevant information is put before the court without defeating the purpose of withholding information in the first place.”¹¹

- 12.8.3 As an aside, and unconnected with section 119, there has been a Complaints Review Tribunal case in which evidence was heard by the Tribunal *in camera* in the absence of the plaintiff. In *O v N (No 2)*¹² the plaintiff was seeking the identity of “X” referred to in a psychologist’s report. To assist the Tribunal I made the suggestion, which was acted upon, that the Tribunal should initially consider whether there was good reason under section 29(1)(b) to withhold information before seeking information as to who X was. If it had been held that there was good reason to withhold then the problem of how to receive evidence from or about X, without disclosing material tending to identify X to the plaintiff, could be avoided.
- 12.8.4 In fact, the Tribunal determined that it was necessary to consider evidence of X’s identity and therefore developed a means for hearing the evidence. The Tribunal developed a draft practice note based upon the practice of the Australian Administrative Appeals Tribunal which it provided to the parties for comment. Later the Tribunal convened a hearing in the absence of the plaintiff and the plaintiff’s representative to hear from the Commissioner’s counsel about what the Commissioner knew of X and why the Commissioner was of the opinion that X’s name should be withheld. The Tribunal considered that information and ruled in the plaintiff’s presence that the hearing would be adjourned for the rest of the day and that it would receive evidence from X in the plaintiff’s absence. The evidence was received in the presence of the Commissioner’s counsel.

12.9 SECTION 120 - Adverse comment

- 12.9.1 This provision requires the Commissioner, when proposing to make a comment that is adverse to another person, to give the person concerned a chance to present his or her side of the matter. The provision is derived from section 78(2) of the (now repealed) Human Rights Commission Act 1977 and continues section 32 of the Privacy Commissioner Act 1991.
- 12.9.2 The provision has its main relevance in respect of my functions in relation to complaints although it occasionally arises in other contexts as well.¹³ The practice I have adopted in relation to complaints which have not proved possible to settle is to write a provisional opinion which is given to the party to which it is adverse. That party is given a reasonable opportunity to respond and, if the complaint is not settled in the meantime, I either confirm my opinion as final or reconsider it in the light of representations made. In fact, because of the nature of the jurisdiction, I commonly render opinions which are adverse in

¹¹ *Freedom of Information in New Zealand*, 1992, page 594.

¹² (1996) 3 HRNZ 636

¹³ I have for example sometimes shown drafts of reports, or public statements, that I have intended to make to certain parties in this vein.

some respect to one party yet favourable in another. This is particularly the case where a complaint raises issues under several information privacy principles or where several grounds are relied upon to withhold information. In such cases a provisional opinion, in different terms, is rendered to each party.

- 12.9.3 The complaints process itself is an inquisitorial one and the *audi alteram partem* rule does not apply. It is therefore important that the party has an opportunity to comment, not during the process of investigation, but at the point when the Commissioner is about to come to an opinion. The procedure is adopted because of its advantages to the investigation in ensuring that each party's position has been understood and that the provisional interpretation of the facts by the Commissioner can be addressed.

12.10 SECTION 121 - Delegation of functions or powers of Commissioner

- 12.10.1 The section permits me to delegate to any person holding office under me any of my functions or powers under the Act or under any other Act.

- 12.10.2 In practice I have been sparing in my use of the delegation power. While I have, for instance, delegated the function of rendering opinions on complaints to my Manager Investigations, the power is not generally exercised except when I am unable to fulfil the function personally - for example, where I am out of the country or there may be a perceived conflict of interest.¹⁴ I am satisfied that much of the fine reputation of the Ombudsmen was built on the knowledge that the decisions made were those of the Ombudsmen themselves. Likewise I believe that confidence in the opinions I give may often be derived from the fact that the opinion is that of the Commissioner and not of a deputy or a delegate. Also I have taken the view that in the early years of the Act it is expected that I, as Commissioner, personally give opinions on complaints which may act as precedents (in a general - not legal - sense) for both my office and for agencies. I appreciate with the increase in the volume of complaints a different view may be taken in the future and the Commissioner may delegate the rendering of opinions on certain classes of complaints.

12.11 SECTION 122 - Delegate to produce evidence of authority

- 12.11.1 This provision requires that a delegate of the Commissioner produce evidence, when required to do so, of that person's authority to exercise the Privacy Commissioner's power. This has not caused any difficulties in practice.

12.12 SECTION 123 - Revocation of delegations

- 12.12.1 Section 123 provides that every delegation under section 121 is revocable, at will, in writing. The delegation is to continue in force until revoked, even if the Commissioner who originally made the delegation no longer holds office. No issues have arisen in practice as yet.

12.13 SECTION 124 - Delegation of powers by local authority

- 12.13.1 Sections 124 and 125, which run to almost two pages of the statute, concern delegation of powers by local authorities and by officers of local authorities. In 1997 it was suggested to me that these provisions were unnecessary due to sufficient powers of delegation existing in the Local Government Act 1974. I determined to follow through on this issue since there appeared to me to be an opportunity to "unclutter" the Act if these two lengthy provisions could be omitted. In the discussion paper I posed questions to find out whether local

¹⁴ For example, where a respondent was a company of which I had previously been a director.

authorities considered sections 124 and 125 really necessary or whether they would find it more convenient to have the delegation powers located in the Local Government Act.

12.13.2 In addition to receiving submissions from local authorities, and people knowledgeable about local authority affairs, I invited representatives from local authorities in the Wellington and surrounding regions, Local Government New Zealand and the Department of Internal Affairs to a meeting in December 1997. I obtained a number of valuable comments. A consensus was reached that territorial authorities would find it advantageous to use the delegation powers in the Local Government Act since this is their normal point of reference. Another advantage of repositioning delegation powers is that the Local Government Act establishes a delegation register which is a valuable central reference point. Delegation powers become problematic when they are scattered throughout other pieces of legislation.

12.13.3 Local authorities present at the meeting suggested that section 78 of the Building Act 1991 provided a model for a replacement to sections 124 and 125. That section provides:

“Delegation of powers by territorial authority and its officers - The provisions of sections 715 and 716 of the Local Government Act 1974, with all necessary modifications, shall apply in respect of the powers under this Act of every territorial authority and its officers.”

12.13.4 A provision to replace sections 124 and 125 of the Act, modelled upon section 78 of the Building Act, might appear something like the following:

Delegation of powers by local authority and its officers

- (1) The provisions of sections 715 and 716 of the Local Government Act 1974 apply in respect of the powers under this Act of every local authority that is a council, within the meaning of that Act, and of members and officers of the council.
- (2) The provisions of sections 42 and 43 of the Local Government Official Information and Meetings Act 1987 apply in respect of the delegation of the powers under this Act of every local authority not specified in subsection (1) and of officers and employees of the local authority.

12.13.5 The draft provision is more complex than section 78 of the Building Act as it needs to take account of the fact that not all “local authorities” are “territorial authorities” subject to the Local Government Act. However, those other local authorities are satisfactorily accounted for in the proposed subclause (2).



RECOMMENDATION 147:

Sections 124 and 125 should be repealed and replaced by a single brief provision providing that the relevant delegation provisions in the Local Government Act 1974 and Local Government Official Information and Meetings Act 1987 apply.

12.14 SECTION 125 - Delegation of powers by officers of local authority

12.14.1 Section 125 provides that any officer or employee of a local authority may, by writing, delegate to any other officer or employee any of his or her powers under the Privacy Act, except the power to delegate under section 125 itself. As discussed in relation to section 124, involving delegation of powers by a local

XIII

s 125

357

“Sections 124 and 125 of the Privacy Act are almost identical to the general delegation power under the Local Government Act 1974. Having separate provisions is confusing. We suggest their replacement by a reference to the Local Government Act. (This will have the added benefit of bringing the Privacy Act delegations within the ambit of the delegations register).”

- LOCAL GOVERNMENT NEW ZEALAND, SUBMISSION S51

authority, I believe that this provision may be more briefly stated and the details should primarily be found in local government statutes.

12.15 SECTION 126 - Liability of employer and principals

- 12.15.1 I have already briefly mentioned this provision in the context of section 4 which concerns the actions of, and disclosure of information to staff of an agency.¹⁵ I observed that it is unfortunate that it is necessary for employers and employees to seek out sections in opposite ends of the statute to obtain the complete picture on liability. However, I took the view that if each provision is read a reader will obtain a relatively plain message as to the combined effect.
- 12.15.2 I have had to consider section 126 in a number of cases. In respect of several of these I have issued case notes.¹⁶ The Tribunal has not yet given a decision concerning the interpretation of the provisions. I have no recommendation to change the section.

12.16 SECTION 127 - Offences

- 12.16.1 Unlike many overseas privacy laws, there are very few criminal offences in the Privacy Act. For example, it is not an offence to breach an information privacy principle. Rather, the Act provides for civil remedies. If an agency has caused an interference with the privacy of an individual the Act can provide a resolution to an individual's complaint and, if necessary, compensation or enforceable orders to prevent repetition of the harm. I prefer this approach to any widespread use of the criminal law which would seek to punish an agency. Both approaches are directed towards preventing a repetition of the action but the civil law approach is less "heavy handed" and ensures that the individual, who should be the centre of any privacy process, is given redress if possible. I am not persuaded that it would generally be better to enforce the privacy principles by criminal law sanctions. The purpose of the Act is to improve agencies' practices in respect to personal information. The efficacy of the criminal law approach in this regard is suspect. Indeed, the imposition of criminal liability on such parties can be counter-productive.
- 12.16.2 However, it is appropriate to supplement with certain offence provisions a law which primarily revolves around civil law remedies. An example of this is the existing section 127 which provides for a fine of up to \$2,000 for deliberately obstructing or misleading the Commissioner. I believe that the addition of some further and suitably crafted offences will make the legislation more effective. However, I have been cautious in recommending such measures since I continue to believe that the present civil approach continues to be the most appropriate. The recommendations I make for new offences revolve around areas where the civil law is simply not up to the task constraining certain wilful and unacceptable behaviour which has serious social consequences.

Discussion paper and submissions

- 12.16.3 In the discussion paper I sought comments upon the general approach to be taken in introducing new offence provisions into the Act as well as seeking comments upon two specific offence provisions I had been considering.
- 12.16.4 Submissions were divided on whether it is appropriate to consider introducing new offence provisions into an Act largely based on civil remedies. However, there was strong support for specific offence provisions where a person intentionally misleads an agency into giving access to information by impersonating the individual concerned or misrepresenting authorisation from that person.

¹⁵ See paragraph 1.6.

¹⁶ See case notes 3734, 6998 and 14824.

“The Group sees the issues as concerning the extent to which the criminal law is the appropriate means of providing incentives to comply with the Act. Where the matter raises questions of the public interest, or where there is a need to constrain truly dishonest or criminal behaviour (eg. knowingly impersonating an individual to make an access request for pecuniary gain) then there is a legitimate involvement of the criminal law.”

- NZ LAW SOCIETY PRIVACY WORKING GROUP, SUBMISSION G22

Similarly, there was support for creating a specific offence of knowingly destroying information to which a person is entitled to have access in order to deny the person that right. There was also support for including computer crimes such as hacking in the Privacy Act, with a number of submissions preferring such offences to be placed elsewhere such as the Crimes Act.

Impersonating the individual concerned

- 12.16.5 The first new offence that I recommend be created concerns the actions of any person who knowingly makes a request for access to, or correction of, personal information under false pretences. This proposal reflects, in part, the fact that the Privacy Act has obliged agencies in the private sector to open up their files to individuals where previously they may have kept them far more securely closed to outsiders. In such circumstances the agency is put at risk, as is the privacy of the individual concerned, if a person impersonates the individual entitled to have access or misrepresents the position by falsely claiming to have authorisation to have access to information.
- 12.16.6 Presently, the only remedy for the aggrieved individual is to take a complaint against the agency. At best, the individual may obtain redress from the duped agency for disclosure of information or a failure to take reasonable security safeguards, but may well obtain no redress because the security safeguards were, in the circumstances, adequate. Typically there will be no recourse under the Privacy Act against the individual who had deliberately misrepresented the position. In many cases the individual who has used false pretences to obtain the information can take advantage of the domestic affairs exemption in section 56 of the Act if they can show that they collected the information in connection with their personal, family or household affairs.
- 12.16.7 Many businesses feel vulnerable to such deception. Yet there has to be a sensible standard regarding security safeguards to ensure that business and government can operate efficiently. A person who steals an object of value or obtains it by false pretences commits an offence. Access to personal information may sometimes have considerable value but, whether it does or not, the law needs to make plain that obtaining it by deception is not acceptable in any circumstances.
- 12.16.8 This issue is addressed in other jurisdictions. The Australian Privacy Act, for instance, provides that a person must not, by a false pretence, obtain access to an individual's credit information file or credit report in the possession or control of a credit reporting agency. The penalty for breach is a \$30,000 fine¹⁷. The Hong Kong Personal Data (Privacy) Ordinance creates an offence in respect of a person who, in a data access or correction request, supplies information which is false or misleading in a material particular for the purpose of having the data users concerned comply with the request.¹⁸ The offence carries a fine and imprisonment. The Privacy Act 1974 (USA) provides that any person who knowingly or wilfully requests or obtains any record concerning an individual from an agency under false pretences shall be guilty of a misdemeanour carrying a maximum \$5,000 fine.



RECOMMENDATION 148

There should be an offence provision created concerning any person who intentionally misleads an agency by:

- (a) impersonating the individual concerned; or**
(b) misrepresenting the existence or nature of authorisation from the individual concerned;

in order to make the information available to that person or another person or to have the personal information used, altered or destroyed.

¹⁷ Privacy Act 1988 (Australia), section 18T.

¹⁸ Personal Data (Privacy) Ordinance 1995 (Hong Kong), section 64(2).

“The Association considers new offence provisions are warranted for individuals deliberately misleading agencies for the procurement of information. The Association is concerned that a significant number of complaints against banks involve inadvertent release of information to third parties, such as former spouses, who have misled the banks in deliberately seeking such information.”

- NZ BANKERS' ASSOCIATION,
SUBMISSION S40

Destroying requested information to deny access

- 12.16.9 A second offence that I recommend relates to the actions of any person who destroys personal information which has been requested by the individual concerned in order to deny that individual the entitlement to have the request determined or reviewed. It is not intended that this offence extend to agency policies which are to destroy documentation, such as job applications, promptly following the awarding of a position to a successful candidate even though such policies may, in part, be motivated by a wish not to have to hold records available for access. Rather, the offence is directed towards circumstances where an individual requests access and the agency, through a pre-existing policy or through the actions of a person within the agency, destroys the records so that a response may be given that the information does not exist.
- 12.16.10 The reason for proposing such an offence is that in essence the civil law response, involving a complaint and a review of the documents, has been deliberately thwarted. While theoretically it is sometimes possible for the matter to be determined in the absence of the information this is usually quite difficult and sometimes impossible. In any case, the access review in such cases is primarily directed towards seeking to establish what the information was and whether it was properly withheld. The proposed offence focuses upon the reprehensible conduct which would deny individuals their entitlements. Such actions should not be permitted notwithstanding that all or part of the information might have been properly withheld.
- 12.16.11 It may be difficult to undertake such prosecutions. However there are often honest employees within agencies who are disturbed at instructions to destroy records in such circumstances who may act as “whistleblowers”. The existence of such an offence will be apparent to privacy officers and people administering the Privacy Act. It will, no doubt, be referred to in staff training. Management in agencies will find it difficult to give instructions to destroy records in such circumstances since their employees will be unwilling to carry them out.
- 12.16.12 A precedent for such an offence is to be found in the privacy statute in Alberta.¹⁹ This provides that a person must not “wilfully destroy any records subject to the Act with the intent to evade a request for access to the records”.

**RECOMMENDATION 149**

There should be an offence created of knowingly destroying documents containing personal information to which the individual concerned has sought access in order to evade an access request.

Computer crimes

- 12.16.13 Commentators have suggested for many years now that New Zealand’s criminal laws are inadequate in so far as they relate to “hacking” into computer systems. Seven years ago, the Crimes Consultative Committee noted that:

“Computers are now used very widely in our society, yet the traditional property offences cannot deal adequately with misconduct in respect of computers and the information stored on them. New Zealand has fallen behind the United Kingdom and Australia in not having specific legislation relating to computers”²⁰.

- 12.16.14 New Zealand’s law has continued to fall behind as no computer crimes have been enacted since the Crimes Consultative Committee Report. Meanwhile malicious persons may continue to hack into computer systems to view and

¹⁹ Freedom of Information and Protection of Privacy Act 1994 (Alberta), section 86(1)(e).

²⁰ Report of the Crimes Consultative Committee, *Crimes Bill 1989*, April 1991, pages 74-75.

obtain information to which they are not entitled and, on occasion, to cause mayhem. In a recent overseas example it was reported:

“On 27 March [1998] in the District Court in Sydney, [S] was sentenced to three years imprisonment for offences under the Commonwealth Crimes Act computer misuse provisions. [S] had earlier pleaded guilty to charges of inserting data into a computer and unlawful access to computer data.

“According to reports, [S] had hacked into AUSNet’s computer network two months after he was refused a job with the company. [S] altered the company’s home page and published credit card details of identified individuals.

“The incident is said to have cost the company more than \$2 million in lost clients and contracts, and the widespread publicity had contributed to a general lack of consumer and business confidence in the security of the Internet.”²¹

12.16.15 The Crimes Consultative Committee supported the creation of offence provisions concerning the accessing of a computer for dishonest purposes and damaging or interfering with a computer system. The discussion paper asked whether the Privacy Act should include any computer crimes such as hacking into a computer in order to obtain access to personal information or to manipulate such information. Most of the responses offered support for the creation of computer offence provisions but not all saw the Privacy Act as the appropriate vehicle.²²

12.16.16 Privacy may be enhanced by the existence of appropriate computer-based criminal sanctions but I am not convinced that the Privacy Act is the appropriate vehicle to create such offence provisions. There is information besides personal information which the creation of offences would protect. Hackers have the potential to undermine information security and privacy through their activities and the Privacy Act’s principles and complaints mechanisms alone cannot provide an appropriate response. The main focus of the Act is the obligations on agencies which hold information whereas the focus of computer crimes laws would be the actions of hackers. The existence of offence provisions would provide a deterrent to such activity. I urge the enactment of offences such as those recommended by the Crimes Consultative Committee.

Time for laying information

12.16.17 Section 14 of the Summary Proceedings Act 1957 states:

“Except where some other period of limitation is provided by the Act creating the offence or by any other Act, every information for an offence (other than an offence which may be dealt with summarily under section 6 of this Act) shall be laid within six months from the time when the matter of the information arose.”

12.16.18 Accordingly, a prosecution for any of the offences presently listed in section 127, or those proposed to be created, must be commenced within six months.

²¹ “Setting an example - Internet hacker sentenced”, *4/10 Privacy Law & Policy Reporter*, March 1998, page 200.

²² Of 19 respondents, virtually all were in favour (or appeared to be) of a proposition that the Privacy Act include computer offence provisions in it. 12 submissions explicitly supported the proposition - G1, G2, G4, G6, G8, S13, S21, S36, S42, S45, S46 and S54. Of the remaining 7 submissions all but two supported the creation of an offence provision but opposed the use of the Privacy Act as a vehicle for doing so - G10, G12, G21, G22 and S2. One opposed the proposition that there be such computer crimes (G18) and the other favoured a civil, not criminal, response (G5).

“While WCC believes there needs to be offence provisions for computer crimes such as hacking, it is debatable whether the Privacy Act is the best place. The Crimes Act may be a more logical place as it should apply to all hacking, rather than just for personal information.”

- WELLINGTON CITY COUNCIL,
SUBMISSION G12

On the two occasions over the last few years where I have referred a matter to the Police for prosecution it has been outside the 6 month limitation period and the prosecution could not be brought. One such case concerned a refusal to comply with a lawful requirement of the Commissioner in the course of a complaint. In that instance the requirement was able to be reissued and the matter was thereby resolved. The other concerned an individual who impersonated an investigator from my office which was only discovered outside the limitation period. Clearly the offending might not be revealed within 6 months.

- 12.16.19 In addition, with the present lengthy complaints queue I am concerned that cases of deliberately destroying information or evidence or misleading my investigation may not be uncovered until many months after the event and that the Summary Proceedings Act limitation period may cause difficulties. I recommend that a 12 month limitation period be substituted.



RECOMMENDATION 150

Section 107 should provide that every information for an offence must be laid within 12 months from the time when the matter of the information arose.

12.17 SECTION 128 - Regulations

- 12.17.1 The Governor-General may make regulations in connection with the operation and administration of the Privacy Act. To date, one set of regulations has been made under the Act: the Privacy Regulations 1993. These provide for the service and giving of notices and other documents for the purposes of the Privacy Act and are issued pursuant to section 128(a).
- 12.17.2 The Complaints Review Tribunal Regulations 1996 are also relevant to Privacy Act proceedings although they are not issued under the Act.²³ These prescribe procedural requirements in respect of the hearing of proceedings under sections 82 and 83 of the Privacy Act as well as proceedings under the Human Rights Act 1993 and the Health and Disability Commissioner Act 1994.
- 12.17.3 In addition to the regulation making powers conferred under section 128, the Governor-General may by Order in Council:
- amend the Second Schedule by adding any item to the public register provisions (section 65);
 - amend the information matching rules in the Fourth Schedule in accordance with the recommendations of the Privacy Commissioner (section 107); and
 - until the power expired on 1 July 1997, amend the Fifth Schedule, which relates to law enforcement information, on the advice of the Minister of Justice given after consultation with the Privacy Commissioner (section 113).
- 12.17.4 In other parts of the report I have made certain proposals which might be implemented through the creation of new regulations. These may need explicit new specific regulation-making powers to be inserted into section 128.

12.18 SECTION 129 - Amendments, repeals and revocations

- 12.18.1 Section 129:
- amended the enactments specified in the Sixth Schedule;
 - repealed the enactments specified in the Seventh Schedule; and
 - revoked the orders specified in the Eighth Schedule.
- 12.18.2 The amendments to sections specified in the Sixth Schedule:
- omitted references to the Wanganui Computer Centre Act 1976 and related references to the Wanganui Computer Centre itself;

²³ The 1996 regulations replaced the Complaints Review Tribunal Regulations (No. 2) 1993.

- inserted references to section 105B of the Crimes Act in certain statutes referring to bribery and corruption where these presently refer to section 105A;²⁴
- substituted Privacy Act references for those relating to the Privacy Commissioner Act 1991;
- removed references to the Wanganui Computer Centre Privacy Commissioner as an Officer of Parliament.

12.18.3 The statutes repealed in the Seventh Schedule included:

- the Wanganui Computer Centre Act 1976 (together with subsequent amendments and various references in other statutes);
- the Privacy Commissioner Act 1991 (together with various references to that in other statutes).

12.18.4 The revoked orders in the Eighth Schedule were all made pursuant to the Wanganui Computer Centre Act.

12.18.5 One apparently unforeseen result of the repeal of the Wanganui Computer Centre Act was the diminution of access and correction rights for non-New Zealanders. This is discussed in relation to section 34.²⁵

Repeal of Wanganui Computer Centre Act

12.18.6 One particular consequence of the repeal of the Wanganui Computer Centre Act which has had a deleterious effect on privacy has been the repeal of the offence provision that was contained in section 29(2)(c). That provided:

“Every person commits an offence and is liable on conviction on indictment to imprisonment for a term not exceeding two years who requires any person to obtain under section 14 of this Act, or to produce, for any reason whatsoever, or penalises any person for failing to so obtain or produce, a copy from the computer system of all or a part of the law enforcement information that the person is entitled to receive, or has received, upon an application under section 14 of this Act.”

12.18.7 This provision essentially outlawed what may be referred to as “coerced access requests” or “coerced authorised disclosures” of criminal history information, that is the information concerning existence or absence of convictions, and the details of any conviction.²⁶ It was anticipated that with the repeal of the 1976 Act there would be some administrative changes in obtaining access to criminal history information²⁷ but otherwise things would largely remain the same albeit with “Wanganui” access rights subsumed within principle 6 rights. The extensive list of offences in the Wanganui Computer Centre Act - the one quoted is amongst 10 offences in that section - were not continued as they were seen as generally incompatible with the scheme of the Privacy Act which places the emphasis on civil remedies rather than criminal prosecutions.

²⁴ Section 105B, which was part of the package of reforms made by the select committee which studied the Privacy of Information Bill, is discussed in relation to section 118 at paragraph 12.7.

²⁵ See paragraphs 5.3.1 - 5.3.16 and recommendation 61.

²⁶ A coerced access request would be where, say, a prospective employer insists that an applicant make an access request to an agency and deliver the results to the employer. From the perspective of the law enforcement agency it appears the same as any other access request. The enforced authorised disclosure would have the prospective employer require the applicant to sign a form authorising the law enforcement agency to disclose directly to the employer. This differs from an ordinary access request.

²⁷ Most notably, access requests would not be lodged with the Wanganui Computer Centre Privacy Commissioner but with the relevant law enforcement agency or agencies themselves.

- 12.18.8 Unfortunately, there has been a rapid and undesirable rise in coerced requests and authorised disclosures. Both types of requests were unlawful under the Wanganui Computer Centre Act although those of the first type were difficult to detect. The second are plain enough. Figures supplied by the Department for Courts make it plain that there has been a huge growth in requests for criminal history information including of the second type for which there were none prior to 1 July 1993.
- 12.18.9 The Department for Courts presented statistics showing a significant rise in the number of requests for the release of criminal history information, including a doubling of requests in some months between 1996 and 1997.²⁸ The Department observed that a greater number of employers, particularly those involved in the financial and insurance sectors, are seeking criminal conviction checks. The Department anticipated that the Financial Advisers Disclosure Act 1997 would increase the number of requests, which it estimated as increasing at a rate of 20% per year.
- 12.18.10 The Department had presented the material primarily to explain its difficulties in processing so many access requests and the costs that it believed it had to absorb. However, the position is far more worrying from a privacy perspective. The Department confirmed that *only 25% of requests to the Department for criminal history information come from individuals with the remaining 75% originating from third parties such as insurance companies and prospective employers.*²⁹ I expect that the increasing number of access requests from individuals may also be attributed to third party demands (that is, coerced access requests) since access rights have existed since 1977 and might be expected to increase only modestly if driven solely by the interest of the individuals themselves.
- 12.18.11 This offers a dramatic illustration of the rapid establishment and escalation of coerced access requests and coerced authorised disclosures. It would appear plain that three-quarters of the public releases of criminal history information by the Department would not have been permitted under the 1976 Act. The change has not been positive for privacy and it is worrying that, without some change in the law or administrative practice, the rate of disclosure will likely increase even further. There are a variety of privacy concerns in relation to the coerced release of criminal history information. One particular problem with the present New Zealand arrangements is that the Department for Courts has a practice of releasing a list of all convictions regardless of whether the requester simply wishes to have confirmation of the existence of, or details relating to, a class of convictions or convictions since a certain date. This in itself gives rise to an issue in relation to the disclosure of irrelevant information, the release of which has neither been requested nor authorised.
- 12.18.12 There is not even a cost constraint on prospective employers and insurance companies given that the Department is characterising authorised disclosures as information privacy requests and accordingly providing the information without charge.³⁰ Some private investigators are advertising services which imply they offer an investigation into criminal records but which require the prospective employee to make the access request.
- 12.18.13 It is true that there are interests which compete with privacy in the context of the disclosure of criminal history information. It would be possible to devise alternative schemes, involving vetting or clearance certificates which would provide more satisfactory practices regarding release of information where war-

²⁸ Submission S33.

²⁹ Letter Department for Courts to Office of the Privacy Commissioner, 24 November 1997.

³⁰ Privacy Act, section 35(1), prohibits public sector agencies from making a change for an information privacy request.

ranted in the public interest. My concern in this context is that a dramatic change has resulted which was not preceded by any public debate or clear Parliamentary intention. Instead, I understand that it was anticipated that things would continue much as they have before albeit that the Privacy Commissioner would no longer be the entry point for seeking access to Wanganui Computer information.

12.18.14 I recommend that provision be made to reinstate special controls on individual access rights to criminal history information to ensure that information is only released directly to the individual concerned. Disclosure to third parties, such as insurance companies or prospective employers, should only be permitted where there is both:

- express legislative authorisation; and
- written authorisation from the individual concerned.

12.18.15 Specific authority could be provided in an Act, or regulations, providing for the disclosure to a third party where the objectives of that legislation required. For example, in respect of the Financial Advisers Disclosure Act, mentioned in the departmental submission, there would be a need to:

- identify the relevant convictions (for instance, crimes of dishonesty);
- identify the institutions entitled to have such conviction information (for instance, employers of financial advisers);
- prescribe a form and procedure whereby the individual gives written authorisation to the institution to obtain the relevant details.

12.18.16 As well as having benefits for privacy, this approach would likely smooth implementation of initiatives, such as the screening of financial advisers, and thereby make it more effective. The legislation could also establish fees so that the costs are borne by industry or the Government, as appropriate to the particular proposal, and not publicly subsidised by disguising the process as individuals seeking access to their information under information privacy principle 6. That approach would be consistent with the approach recommended by the International Labour Organisation in the employment context. In its recent commentary to a code of practice on the protection of workers' personal data the ILO states:

“As far as criminal convictions are concerned, collection should again be strictly confined to data clearly relevant to the particular employment. For example, in the case of employment involving child care or work with children, a person previously convicted of child molesting should be obliged to expose the fact. A professional driver could likewise be required to disclose information on previous drunk driving convictions. Data about convictions should be obtained directly from the person concerned so as to ensure that only pertinent information is collected. For the same reason, employers should not be allowed to ask workers to provide a copy of their conviction records.”³¹

12.18.17 There has been concern in Britain at the issue of coerced access requests and a provision has been included in the new Data Protection Bill to prohibit the practice. The clause provides in part:

“Prohibition of requirement as to production of certain records

- (1) a person must not, in connection with:
- (a) the recruitment of another person as an employee;

“The Department has some indication that some private investigators and insurance companies are requesting information on criminal convictions with a falsified authorisation signature or a photocopy of that signature from another document.”

- DEPARTMENT FOR COURTS,
SUBMISSION S33

³¹ International Labour Office, *Protection of Workers' Personal Data*, an ILO code of practice 1997, pages 31-32.

- (b) the continued employment of another person; or
 - (c) any contract for the provision of services to whom by another person;
- require that other person or a third party to supply him with a relevant record or to produce a relevant record to him.
- (2) A person concerned with the provision (for payment or not) of goods, facilities or services to the public or a section of a public must not, as a condition of providing or offering to provide any goods, facilities or services to another person, require that other person or a third party to supply him with a relevant record or to produce a relevant record to him.
 - (3) Subsections (1) and (2) do not apply to a person who shows:
 - (a) that the imposition of the requirement was required or authorised by or under any enactment, by any rule of law or by the order of a court; or
 - (b) or that in particular requirements that the imposition of the requirement was justified as being in the public interest.
 - (4) Having regard to the provisions of Part V of the Police Act 1997 (Certificates of Criminal Records etc), the imposition of the requirement referred to in subsection (1) or (2) is not to be regarded as being justified as being in the public interest on the ground that it would assist in the prevention or detection of crime.
 - (5) A person who contravenes subsection (1) or (2) is guilty of an offence.”³²

A table is set out which lists certain criminal history information, as “relevant records” notably convictions and cautions.



RECOMMENDATION 151

A provision should be included to prohibit employers, prospective employers, and providers of services, requiring individuals to exercise their access rights to obtain criminal history information as a condition of obtaining employment, continuing employment, or obtaining services.

Coerced access requests - medical records

- 12.18.18 The problem of coerced access requests, and coerced authorised disclosure, has been manifested primarily in relation to criminal history information. This is the area in which the operation of the Privacy Act has, in a sense, created the problem through the repeal of the Wanganui Computer Centre Act 1976. However, it is not the sole area in which the issue arises. In societies of our type there has been growing problem of employers and insurance companies insisting upon individuals exercising access rights to their health records and delivering a copy to the employer or the insurer. This differs from the practice of employers or insurance companies requiring an individual to undergo a medical examination by the employer’s or insurer’s medical practitioner - a practice which is not of concern in this context. The new UK Bill has tackled this issue with a clause which provides:

“Avoidance of certain contractual terms relating to health records

- (1) Any term or condition of a contract is void in so far as it is purports to require an individual to supply any other

³² Data Protection Bill [HL] (UK), 4 June 1998 version, clause 56(1)-(5).

- person with a record to which this section applies, or with a copy of such a record or a part of such a record.
- (2) This section applies to any record which:
- (a) has been or is to be obtained by a data subject in the exercise of the right conferred by section 7; and
 - (b) consists of the information contained in any health record as defined by section 68(2).³³

Clause 68 defines “health record” to mean any record which:

- (a) consists of information relating to the physical or mental health or condition of an individual; and
- (b) has been made by or on behalf of a health professional in connection with the care of that individual

12.18.19 The problem of coerced access, and coerced authorised disclosure, will continue to grow especially as insurance enters further aspects of our national life. Already, over the last several years, a greater interest by employers has been shown in the health records of their employees as a result of the experience rating system adopted since 1992 in the accident compensation legislation. It is appropriate to have a similar provision to the UK clause in our own Act or at least allow for the same effect to be achieved in a code of practice.



RECOMMENDATION 152

Provision should be made to constrain contractual requirements that oblige individuals to supply copies of health records.

12.19 SECTION 130 - Final report of Wanganui Computer Centre Privacy Commissioner

12.19.1 Section 130 provided for the final report of the Wanganui Computer Centre Privacy Commissioner. The provision was necessary because the final report was submitted after the repeal of the Wanganui Computer Centre Act 1976 pursuant to which previous annual reports were filed. Since the Wanganui Computer Centre Privacy Commissioner was no longer an Officer of Parliament there was no jurisdiction for a report to be presented directly to Parliament. Instead, provision was made for the final report to be submitted to the Minister of State Services who subsequently laid the report before the House of Representatives.

12.19.2 The report was made by P L Molineaux in 1993 and the provision is now spent.³⁴

12.20 SECTION 131 - Privacy Commissioner to complete work in progress of Wanganui Computer Centre Privacy Commissioner

12.20.1 This provision empowered me as Privacy Commissioner, to complete the work in progress of the Wanganui Computer Centre Privacy Commissioner. I reported on the work undertaken in that capacity in my 1993/94 and 1994/95 annual reports.³⁵

12.20.2 At the start of the 1993/94 year there were nine complaints still under investigation. At the beginning of the 1994/95 year seven remained under investigation but all were concluded by the end of that year.

12.20.3 With the repeal of the Wanganui Computer Centre Act 1976 it was also neces-

³³ Data Protection Bill [HL] (UK), 4 June 1998 version, clause 57.

³⁴ See *Final Report of the Wanganui Computer Centre Privacy Commissioner for the year ended 30 June 1993*, AJHR, A4.

³⁵ See *Report of the Privacy Commissioner for the year ended 30 June 1994*, page 12, and *Report of the Privacy Commissioner for the year ended 30 June 1995*, page 13.

sary for me to review the status of the files of the former Wanganui Computer Centre Privacy Commissioner. The review was completed during the 1993/94 year in consultation with the Chief Archivist. Some files were transferred for archiving and some were destroyed.

12.21 SECTION 132 - Savings

12.21.1 Section 132 provides that, for the avoidance of doubt, and without limiting the Acts Interpretation Act, the repeal of the Wanganui Computer Centre Act shall not affect:

- the continuing existence of the Wanganui Computer Centre;
- the computer system established in connection with that computer centre;
- or
- any agreements or arrangements entered into by the Minister of State Services pursuant to section 3A of that Act.

12.21.2 I expect that that provision was included out of an abundance of caution and was actually entirely unnecessary. It is interesting to note that the “continuing existence” of the Wanganui Computer Centre is now mainly in the collective national psyche given that the computer systems formerly operated out of Wanganui are now located somewhere in Auckland. Furthermore, all law enforcement agencies are now in the process of “migrating” away from the Law Enforcement System or are planning to do so by the year 2000. Out of an abundance of caution section 132 provides that the repeal of the Wanganui Computer Centre Act does not affect the continuing existence of the Wanganui Computer Centre - but does its physical removal? Does the fact that law enforcement agencies are ceasing to use it affect its continuing existence? When exactly *does* a computer system cease to exist?

12.21.3 I take the view that section 132 was probably never needed. If it was, its need has now passed. As a tidying up exercise to remove “clutter” from the Act I would like to see section 132 repealed. It may also be undesirable to have two sections of the Act (sections 7 and 132) carrying the same marginal note “savings”.



RECOMMENDATION 153

Section 132 should be repealed.

12.22 SECTION 133 - Transitional provisions

12.22.1 The transitional provision contained in section 133 was necessary because of my appointment under the Privacy Commissioner Act 1991. This provision converted that into a continuing appointment under the current Act.

Summary of Recommendations

R

1. PRELIMINARY PROVISIONS



RECOMMENDATION 1

PAGE 30

The relevant changes in legislative drafting styles recently adopted by the Parliamentary Counsel Office should be applied throughout the Privacy Act. (See paras 1.2.13 - 1.2.15)



RECOMMENDATION 2

PAGE 32

The marginal notes and headings in the following principle, sections, Part and rule should be amended to make them more helpful, accurate and precise: principle 9; sections 7, 27, 28, 42, 45, 73, 95, 100, 101 and 105; Part X; information matching rule 8. (See paras 1.2.16 - 1.2.23)



RECOMMENDATION 3

PAGE 33

The present section notes concerning the official information legislation should be presented in a comparative table at the end of the Act. (See paras 1.2.26 - 1.2.28)



RECOMMENDATION 4

PAGE 33

The Parliamentary Counsel Office should be requested to arrange for a consolidated reprint of the Privacy Act following the implementation of reforms adopted as a result of this report. (See para 1.2.29)



RECOMMENDATION 5

PAGE 37

An appropriate committee of Parliament should consider whether it is desirable to grant individuals access rights to information held about them by the House of Representatives or to adopt rules similar to any of the 12 information privacy principles. (See paras 1.4.15 - 1.4.20)



RECOMMENDATION 6

PAGE 39

An appropriate committee of Parliament should consider whether it is desirable to:

- (a) adopt any measures to encourage members of Parliament to apply, or follow, any of the 12 information privacy principle; or
- (b) provide that MPs in their official capacities are agencies for some purposes of the information privacy principles. (See paras 1.4.27 - 1.4.28)



RECOMMENDATION 7

PAGE 40

Consideration should be given to whether it is appropriate to replace the total exemption for the Parliamentary Service Commission in subparagraph (b)(v) of the definition of “agency” with a partial exemption. (See paras 1.4.29 - 1.4.32)






RECOMMENDATION 8

PAGE 40

The partial exemption for the Parliamentary Service in subparagraph (b)(vi) of the definition of “agency” should be repealed, or further restricted, if this can be achieved in a manner that does not impact upon the exemption in subparagraph (b)(iv). (See paras 1.4.29 - 1.4.32)

-  **RECOMMENDATION 9** PAGE 42
 Consideration should be given to including a definition of “tribunal” limited to statutory tribunals forming part of the New Zealand administrative or judicial structure. (See paras 1.4.40 - 1.4.41)
-  **RECOMMENDATION 10** PAGE 43
 Subparagraph (b)(ix) of the definition of “agency” should be repealed so that the Ombudsmen are considered to be an “agency” for the purposes of the Act. (See paras 1.4.43 - 1.4.48)
-  **RECOMMENDATION 11** PAGE 48
 Consideration should be given to adopting a new definition of “document” in section 2 in conjunction with any redefinition of the term in the proposed Evidence Code. (See paras 1.4.71 - 1.4.73)
-  **RECOMMENDATION 12** PAGE 49
 Consideration should be given to amending the definition of “personal information” to clarify the position of information sourced from, but not contained in, the register of deaths. (See para 1.4.80)
-  **RECOMMENDATION 13** PAGE 50
 Consideration should be given to redefining or recasting “public sector agency”, “Minister”, “department”, “organisation” and “local authority”. (See paras 1.4.82 - 1.4.86)
-  **RECOMMENDATION 14** PAGE 51
 Consideration should be given to enacting a definition of “private sector agency”. (See paras 1.4.87 - 1.4.88)
-  **RECOMMENDATION 15** PAGE 52
 The definition of “statutory officer” should be moved from section 2(1) into section 3. (Refer para 1.4.98)
-  **RECOMMENDATION 16** PAGE 55
 Consideration should be given to the desirability of enacting a definition of “use” which will encompass the retrieval, consultation or use of information. (See paras 1.4.103 - 1.4.111)
-  **RECOMMENDATION 17** PAGE 55
 Section 2(2) should be replaced with a more concise provision. (See paras 1.4.112 - 1.4.113)

2. INFORMATION PRIVACY PRINCIPLES

-  **RECOMMENDATION 18** PAGE 66
 Section 46(4) should be amended to provide that a code of practice may require an agency to take all practicable steps to ensure that an individual may ascertain the agency’s policies and practices in relation to particular personal information. (See paras 2.5.5 - 2.5.8)
-  **RECOMMENDATION 19** PAGE 67
 Information privacy principles 1, 3(1) and 8 should be amended to substitute the phrase “purpose or purposes” for the word “purpose”. (See paras 2.5.10 - 2.5.12)
-  **RECOMMENDATION 20** PAGE 67
 Information privacy principle 3(4)(a) should be repealed. (See paras 2.5.17 - 2.5.19)

-  **RECOMMENDATION 21** PAGE 70
Information privacy principle 3(4)(f)(ii) should be repealed. (See paras 2.5.20 - 2.5.24)
-  **RECOMMENDATION 22** PAGE 71
Consideration should be given to establishing a judicial warrant process in relation to the use of covert video surveillance in the investigation of offences. (See paragraph 2.6.5)
-  **RECOMMENDATION 23** PAGE 74
Information privacy principle 5(a)(ii) should be amended by inserting the word “browsing” or “inspection”. (See paras 2.7.13 - 2.7.16)
-  **RECOMMENDATION 24** PAGE 76
Information privacy principle 7 should be suitably amended so that agencies are obliged to inform requesters, in cases where the agency is not willing to correct information, that they may request that a statement be attached to the information. (See paras 2.9.6 - 2.9.7)
-  **RECOMMENDATION 25** PAGE 78
Information privacy principle 7 should be supplemented with a right to prevent the use or disclosure of personal information for the purposes of direct marketing through the deletion or blocking of personal information held by the agency for direct marketing purposes. (See paras 2.9.8 - 2.9.15)
-  **RECOMMENDATION 26** PAGE 80
Consideration should be given to amending information privacy principle 8 to substitute the phrase “use or disclose” for “use” in the first line. (See paras 2.10.4 - 2.10.10)
-  **RECOMMENDATION 27** PAGE 84
Section 46(4) should be amended to provide that a code of practice may require an agency to retain specified information or documents for a specified period, not exceeding six years. (See paras 5.11.12 - 5.11.18)
-  **RECOMMENDATION 28** PAGE 91
In relation to the controls on reassignment of unique identifiers:
(a) information privacy principle 12(2) should be limited so that the prohibition is solely in relation to the reassignment of unique identifiers originally generated, created or assigned by a public sector agency; and
(b) section 46(4) should be amended to make it clear that a code of practice may apply the controls in principle 12(2) to the assignment of unique identifiers generated, created or assigned by any agency (not simply a public sector agency). (See paras 2.14.12 - 2.14.17)
-  **RECOMMENDATION 29** PAGE 92
Section 66(1) should be amended so that an interference with privacy may be established notwithstanding the absence of any harm or detriment of the type set out at section 66(1)(b) in cases of wilful breach of information privacy principle 12(2). (See paras 2.14.18 - 2.14.23)
-  **RECOMMENDATION 30** PAGE 95
Section 7(1) should be amended by transferring its content, in so far as it relates to information privacy principle 11, into principle 11 as a new exception. (See paras 2.15.15 - 2.15.19)

**RECOMMENDATION 31**

PAGE 95

Consideration should be given to transferring the content of:

- (a) section 7(4) into information privacy principles 1 to 5, 7 to 10, and 12 as exceptions; and
- (b) section 7(5) into Part VI. (See paras 2.15.15 - 2.15.19)

**RECOMMENDATION 32**

PAGE 96

The content of section 7(2) and (3), in so far as they relate to information privacy principle 6, should be relocated into Part IV. (See paras 2.15.20 - 2.15.21)

**RECOMMENDATION 33**

PAGE 98

Section 7(2) and (3), in so far as they relate to information privacy principle 11, should be repealed and replaced with a single provision, which may be relocated into principle 11 itself, to the effect that where another enactment imposes a more restrictive obligation of secrecy or non-disclosure than principle 11, the principle does not operate to provide additional grounds for disclosure. (See paras 2.15.22 - 2.15.30)

**RECOMMENDATION 34**

PAGE 99

A sunset clause should provide for the expiry of section 7(3) after a period of 3 years. (See paras 2.15.34 - 2.15.38)

**RECOMMENDATION 35**

PAGE 107

The Act should be amended to include express provision for controlling transborder data flows, consistent with clause 17 of the OECD Guidelines and the emerging international approach to data export. In particular consideration should be given to providing:

- (a) a mechanism which would enable mutual assistance to be extended to prohibit data exports in circumstances where New Zealand is being used as a conduit for transfers designed to circumvent controls in EU and other privacy laws;
- (b) mechanisms for imposing restrictions concerning categories of personal information for which there are particular sensitivities and in respect of which the recipient countries would provide no adequate protection. (See paras 2.18.6 - 2.18.20)

**RECOMMENDATION 36**

PAGE 108

Section 11 should be amended so that the entitlement under information privacy principle 6(1) to have access to information held by an agency is a legal right in circumstances where the agency is prosecuting the individual for an offence. (See paras 2.19.4 - 2.19.8)

3. **PRIVACY COMMISSIONER****RECOMMENDATION 37**

PAGE 111

There should be provision for the Commissioner to put a case for funding directly to Treasury and relevant Ministers. (See para 3.2.5)

**RECOMMENDATION 38**


PAGE 132


Section 15(3) should be amended to make clear that a deputy may be designated as an alternate Human Rights Commissioner with the concurrence with the Chief Human Rights Commissioner. (See para 3.5.4)


**RECOMMENDATION 39**


PAGE 134


Section 20(2) should be amended by substituting “Human Rights Act 1993” for the reference to the “Human Rights Commission Act 1977”. (See para 3.10.2)


 **RECOMMENDATION 40** PAGE 134
 Consideration should be given to repealing section 21. Consequently section 13(1)(d) should be repealed and the content of section 21(1)(a) to (f) transferred to a rewritten section 22. (See paras 3.11.4 - 3.11.5)

 **RECOMMENDATION 41** PAGE 135
 Consideration should be given to the costs and benefits of having the Ministry of Justice include some of the information listed in section 21(1) in any future Directory of Official Information. (See paras 3.11.6 - 3.11.9)

 **RECOMMENDATION 42** PAGE 136
 Section 21(3) should be amended so that the Commissioner is obliged to have regard, in determining whether or not a directory of personal information should be prepared, to the compliance costs to agencies consequent upon such a determination. (See paras 3.11.10 - 3.11.11)


 **RECOMMENDATION 43** PAGE 137
 An appropriate amendment should be made to section 21(1) or 22 so that it is plain the Privacy Commissioner has the power to obtain from an agency the identity of the agency's privacy officer to enable the Commissioner to respond to enquiries from the public. (See para 3.12.5)


 **RECOMMENDATION 44** PAGE 138
 Section 23 should be amended to delete the words “within that agency”. (See paras 3.13.5 - 3.13.8)


 **RECOMMENDATION 45** PAGE 140
 Clause 2(3) of the First Schedule should be repealed so that the Minister does not have the function of determining how many staff the Commissioner engages whether generally or in respect of any specified duties. (Refer paras 3.15.4 - 3.15.6)


 **RECOMMENDATION 46** PAGE 140
 Clause 6(2) of the First Schedule should be repealed as being unnecessary. (See paras 3.15.7 - 3.15.8)












4. GOOD REASONS FOR REFUSING ACCESS TO PERSONAL INFORMATION












 **RECOMMENDATION 47** PAGE 148
 The existing reasons for refusal of requests set out in sections 27, 28 and 29 should be reorganised into an ungrouped list of reasons to make it easier for users of the Act to locate relevant provisions. (See paras 4.1.12 - 4.1.20)

 **RECOMMENDATION 48** PAGE 152
 Consideration should be given to the merits of redrafting the “maintenance of the law” withholding grounds to make more plain the constituent law enforcement interests protected. (See paras 4.2.8 - 4.2.19)

 **RECOMMENDATION 49** PAGE 153
 Consideration should be given to the desirability of enabling the withholding of information where there is a significant likelihood of harassment of an individual as a result of the disclosure of information. (See paras 4.2.20 - 4.2.24)

 **RECOMMENDATION 50** PAGE 155
 Section 28(1)(a) should be repealed as being unnecessary as a reason for withholding information. However if it is retained a straightforward definition of “trade secret” should be inserted into the provision. (See paras 4.3.3 - 4.3.8)

-  **RECOMMENDATION 51** PAGE 156
 Consideration should be given to amending section 28(1)(b) to provide for withholding of information where the disclosure would unreasonably prejudice the commercial position of the agency itself, particularly where the information requested would reveal the agency’s bargaining position in respect of negotiations involving the individual concerned. (See paras 4.3.9 - 4.3.13)
-  **RECOMMENDATION 52** PAGE 158
 Consideration should be given to providing statutory guidance on the withholding of information in the common cases of “mixed” information concerning the requester and other individuals. (See paras 4.4.2 - 4.4.7)
-  **RECOMMENDATION 53** PAGE 160
 It should be made clear that section 29(1)(b) is not available in relation to material that is provided by a person within the agency as part of his or her job. (See paras 4.4.13 - 4.4.15)
-  **RECOMMENDATION 54** PAGE 160
 Sections 43 and 44 should be amended so that the grounds in support of the reasons for withholding evaluative material be given, without the requester needing to expressly ask, unless the giving of those grounds would itself prejudice the interests protected by section 29(1)(b). (See paras 4.4.16 - 4.4.19)
-  **RECOMMENDATION 55** PAGE 161
 Section 29(1)(b) should be amended to clarify that the author of evaluative material may refuse an information privacy request in circumstances where the material may be withheld by the recipient agency. (See paras 4.4.20 - 4.4.22)
-  **RECOMMENDATION 56** PAGE 162
 Consideration should be given to amending section 29(1)(c) to provide for consultation with the individual’s medical practitioner or, in the circumstances of the case, the individual’s psychologist. (See paras 4.4.26 - 4.4.31)
-  **RECOMMENDATION 57** PAGE 164
 Section 29(1)(f) should be redrafted so that it provides a self-contained explanation of the meaning of legal professional privilege. (See paras 4.4.39 - 4.4.43)
-  **RECOMMENDATION 58** PAGE 170
 Section 29(2)(c) should be redrafted to make plain the link with the obligations to transfer a request. (See paras 4.4.79 - 4.4.80)
-  **RECOMMENDATION 59** PAGE 172
 Section 31 should be repealed. (See paras 4.6.1 - 4.6.5)
-  **RECOMMENDATION 60** PAGE 174
 Consideration should be given to extending the application of section 32 to information to which section 29(1)(e) applies. (See paras 4.7.5 - 4.7.7)
5. **PROCEDURAL PROVISIONS RELATING TO ACCESS TO AND CORRECTION OF PERSONAL INFORMATION**
-  **RECOMMENDATION 61** PAGE 180
 The standing requirements in section 34 should be abolished. (See paras 5.3.1 - 5.3.16)

-  **RECOMMENDATION 62** PAGE 181
Public sector agencies should be entitled to make a reasonable charge, of the type permitted by section 35, for making information available to an individual overseas who is neither a New Zealand citizen nor permanent resident. (Refer paras 5.3.19 - 5.3.21)
-  **RECOMMENDATION 63** PAGE 181
If the general standing requirement in section 34 is removed then section 13(3) of the Adoption (Intercountry) Act 1997 should be repealed. (See para 5.3.22)
-  **RECOMMENDATION 64** PAGE 184
Section 35 should be redrafted in a simpler fashion. (See paras 5.4.2 - 5.4.3)
-  **RECOMMENDATION 65** PAGE 185
Section 35(3)(b)(i) should be repealed. (See paras 5.4.4 - 5.4.6)
-  **RECOMMENDATION 66** PAGE 188
The Commissioner or the Tribunal should be empowered to exempt an agency from having to deal with a particular individual's access request for a fixed period where it can be shown that the individual has lodged requests of a repetitious or systematic nature which would unreasonably interfere with the operations of the agency and amount to an abuse of the right of access. (See paras 5.4.9 - 5.4.16)
-  **RECOMMENDATION 67** PAGE 190
Section 37 should be amended to make it clear that in cases where a request for urgency has been substantiated, an agency is obliged to make reasonable endeavours to process the request with priority. (See paras 5.6.1 - 5.6.7)
-  **RECOMMENDATION 68** PAGE 193
Section 39 should be amended so that:
(a) an agency is relieved of the obligation to transfer a request in circumstances where it has good reason to believe that the individual does not wish the request to be transferred; and
(b) the agency duly informs the requester, together with information about the appropriate agency to which any future request should be directed. (Refer paras 5.8.2 - 5.8.3)
-  **RECOMMENDATION 69** PAGE 194
Consideration should be given to clarifying the meaning of the phrase "time limit fixed" in section 66(3) so as to emphasise the primary obligation to give access "as soon as reasonably practicable". (See paras 5.9.2 - 5.9.7)
-  **RECOMMENDATION 70** PAGE 195
Section 40(3) and (4) should be repealed. (See paras 5.5.98 - 5.9.11)
-  **RECOMMENDATION 71** PAGE 196
Complexity of the issues raised by a request should be added to the grounds for an extension of time under section 41(1) (See paras 5.10.6 - 5.10.7)
-  **RECOMMENDATION 72** PAGE 197
Section 41(3) should be amended by replacing the phrase "within 20 working days" with "as soon as reasonably practicable, and in any case not later than 20 working days". (See para 5.10.9)

6. CODES OF PRACTICE AND EXEMPTIONS FROM INFORMATION PRIVACY PRINCIPLES



RECOMMENDATION 73

PAGE 209

Section 46(2)(aa) should be amended by deleting all of those words in parentheses, that is “but not all of those principles”. (See paras 6.2.9 - 6.2.11)



RECOMMENDATION 74

PAGE 210

Section 46(4) should be amended by adding a paragraph acknowledging that a code may provide for such other matters as specified in any other Act. (See para 6.2.15)



RECOMMENDATION 75

PAGE 211

Section 46(6) should be replaced with a provision which empowers the Privacy Commissioner to include in a code of practice a provision applying principle 11 to an agency, or a class of agencies, to health information about any deceased person for a period specified in the code beyond any such person’s death. (See paras 6.2.17 - 6.2.21)



RECOMMENDATION 76

PAGE 212

Consideration should be given to amending section 47(3) to make it clear that a body can apply for a code whether it represents the whole of a class of agencies, industry, profession etc or just a substantial section. (See paras 6.3.1 - 6.3.8)



RECOMMENDATION 77

PAGE 213

There should be provision for the Commissioner to require a representative body applicant to undertake notification under section 47(4) in terms directed by the Commissioner. (See paras 6.3.9 - 6.3.12)



RECOMMENDATION 78

PAGE 214

Section 47(5) should be repealed. (See paras 6.3.13 - 6.3.17)



RECOMMENDATION 79

PAGE 220

Section 54(1) should be amended to enable the Commissioner to grant an exemption to enable information to be kept notwithstanding that this would otherwise be in breach of principle 9. (See paras 6.10.6 - 6.10.7)



RECOMMENDATION 80

PAGE 220

Section 54 should provide that the Commissioner may require the applicant to publicly notify an application in appropriate terms. (See paras 6.10.8 - 6.10.9)



RECOMMENDATION 81

PAGE 222

Consideration should be given to the desirability of narrowing section 55(b) so as to enable access requests by the individual concerned to evidence given, or submissions made, to a Royal Commission prior to the report to the Governor-General where that evidence was given, or the submissions made, in open public hearing. (See paras 6.11.6 - 6.11.10)



RECOMMENDATION 82

PAGE 224

Section 56 should be amended so that an individual cannot rely upon the domestic affairs exemption where that individual has collected personal information from an agency by falsely representing that he or she has the authorisation of the individual concerned or is the individual concerned. (See paras 6.12.5 - 6.12.11)




RECOMMENDATION 83

PAGE 229

The exemption for intelligence organisations in section 57 should be narrowed so that principles 1, 5, 8 and 9 apply to information collected, obtained, held, or used, by an intelligence organisation. (See paras 6.13.1 - 6.13.24)

7. PUBLIC REGISTER PERSONAL INFORMATION

-  **RECOMMENDATION 84** PAGE 239
Public register privacy principle 1 should be amended so that search references be required to be consistent with the purpose of a particular register. (See paras 7.4.5 - 7.4.11)
-  **RECOMMENDATION 85** PAGE 240
As new public register provisions are enacted, or existing ones reviewed or consolidated or amended, consideration should be given to including statutory statements of purpose. (See paras 7.4.14. - 7.4.17)
-  **RECOMMENDATION 86** PAGE 241
Consideration should be given to establishing in the Act a regulation-making power to specify, in respect of any particular public register, the purposes for which the register is established and is open to search by the public. (See para 7.4.21)
-  **RECOMMENDATION 87** PAGE 243
Public register privacy principle 2 should be re-enacted with a structure which more clearly leads users to identify its elements. (See paras 7.5.6 - 7.5.7)
-  **RECOMMENDATION 88** PAGE 245
Public register privacy principle 3 should be amended by adding “in New Zealand” after the words “a member of the public”. (See paras 7.6.12 - 7.6.13)
-  **RECOMMENDATION 89** PAGE 246
If recommendation 88 is adopted, there should be a power in the Act to make regulations, after consultation with the Privacy Commissioner, in respect of any public register to authorise and control the electronic transmission of personal data which is not limited to members of the public within New Zealand. (See paras 7.6.12 - 7.6.13)
-  **RECOMMENDATION 90** PAGE 247
Public register privacy principle 4 should be amended so that the constraints upon charging for access to personal information from a public register apply only in relation to the making available of information to the individual concerned. (See paras 7.7.1 - 7.7.4)
-  **RECOMMENDATION 91** PAGE 251
A further public register privacy principle should be enacted that provides that personal information containing an individual’s name, together with the individual’s address or telephone number, is not to be disclosed from a public register on a volume or bulk basis unless this is consistent with the purpose for which the register is maintained. (See paras 7.8.1 - 7.8.15)
-  **RECOMMENDATION 92** PAGE 252
Section 7(6) should be replaced with a subsection in section 8 providing that the information privacy principles apply in respect of a public register only to the extent specified in section 60 and 63(2)(b). (See paras 7.9.6 - 7.9.8)
-  **RECOMMENDATION 93** PAGE 253
Section 60 should be amended as follows:
(a) in subsection (1) omit the phrases “subject to subsection (3) of this section” and “so far as is reasonably practicable”;
(b) the content of subsection (3) should be moved adjacent to subsection (1) and redrafted in plainer fashion;
(c) in subsection (2) “person” should be replaced by “agency”. (See paras 7.9.9 - 7.9.11)

**RECOMMENDATION 94**

PAGE 253

Section 60(2) should be amended:

- (a) by omitting the words “as far as is reasonably practicable”; and
- (b) by substituting an exception based upon the authorisation of the individual concerned. (See paras 7.9.12 - 7.9.13)

**RECOMMENDATION 95**

PAGE 254

The public register privacy principles should be enforceable in a similar manner to the information privacy principles by amending, as necessary, sections 61(3)-(5) and 66. (See paras 7.10.4 - 7.10.6)

**RECOMMENDATION 96**

PAGE 258

The Order in Council process in section 65 should be utilised to add existing register provisions in enactments to the list in the Second Schedule. The Ministry of Justice should commence work to identify the relevant enactments, and to consult with the relevant agencies, so that the first Order in Council is ready to be issued during the 1998/99 year with the completion of the project by the end of the following year. (See paras 7.14.1 - 7.14.7)

**RECOMMENDATION 97**

PAGE 258

The Ministry of Justice should, in carrying out the exercise to bring register provisions into the Second Schedule pursuant to section 65, also consider in respect of each register the desirability of issuing regulations under section 121 of the Domestic Violence Act 1995. (See paras 7.14.9 - 7.14.11)

**RECOMMENDATION 98**

PAGE 264

A new public register privacy principle should be created which obliges agencies maintaining public registers to adopt a process to hold details of an individual's whereabouts separately from information generally accessible to the public where it is shown that the individual's safety or that of the individual's family would be put at risk through the disclosure of the information. An exception is to be provided where alternative safeguards exist to ensure that such information is not disclosed to the public for purposes unrelated to the purposes for which the information was collected or obtained. (See paras 7.15.1 - 7.15.21)

**RECOMMENDATION 99**

PAGE 265

A mechanism should be established in Part VII of the Act, with the details set out in a new schedule, enabling individuals to obtain suppression directions in relation to public registers which would replace Part VI of the Domestic Violence Act but be applicable to a wider range of circumstances concerning personal safety and harassment. (See paras 7.15.22 - 7.15.26)

**RECOMMENDATION 100**

PAGE 266

The official information statutes should be excluded from questions of release of personal information from public registers. (See paras 7.16.1 - 7.16.5)

8. COMPLAINTS

**RECOMMENDATION 101**










PAGE 271

Section 66(1) should be amended by deleting the words “and only if”. (See paras 8.2.1 - 8.2.7)

**RECOMMENDATION 102**

PAGE 272

Section 67(2) and (3) which provide for the lodging of complaints under the Privacy Act with the Ombudsmen, and for the transfer of such complaints, should be repealed. (See paras 8.3.2 - 8.3.3)

-  **RECOMMENDATION 103** PAGE 273
Section 70(2) should be amended so that the Commissioner is obliged to advise of the procedure to be followed only where he has decided to investigate a complaint so as to avoid overlap with the obligations in section 71(3). (See paras 8.6.2 - 8.6.4)
-  **RECOMMENDATION 104** PAGE 275
Section 70 should be amended to recognise that a decision to investigate a complaint, or to take no action on a complaint, may be postponed until preliminary inquiries are made of the complainant for the purpose of determining whether:
(a) the Commissioner has power to investigate the matter;
(b) the Commissioner may, in his or her discretion, decide not to investigate the matter; or
(c) the complainant wishes to proceed with the complaint. (See paras 8.6.6 - 8.6.11)
-  **RECOMMENDATION 105** PAGE 275
Consideration should be given to establishing a process whereby a decision by the Commissioner that a complaint is beyond jurisdiction can, on this question alone, be referred by the complainant to the Complaints Review Tribunal for its decision on the matter. (See paras 8.6.12 - 8.6.14)
-  **RECOMMENDATION 106** PAGE 278
Provision should be made in Part VIII of the Act for the Commissioner to defer action, or further action, on a complaint where:
(a) the complainant has not complained to the agency concerned and the Commissioner considers that the complainant should do so in an attempt to directly resolve the matter; or
(b) the complaint concerns an agency in respect of which there is an independent, expeditious and appropriate procedure for addressing such complaints available through an industry body which the complainant has not used. (See paras 8.7.5 - 8.7.16)
-  **RECOMMENDATION 107** PAGE 280
Sections 72, 72A and 72B should be combined into a single section providing for the referral of complaints to the Ombudsmen, Health and Disability Commissioner and Inspector-General of Intelligence and Security, and consideration should be given to listing other statutory complaints bodies. (See paras 8.8.1 - 8.10.2)
-  **RECOMMENDATION 108** PAGE 282
Adequate funding should be made available so that the volume of complaints received at the Office of the Privacy Commissioner can be processed, as required by section 75, “with due expedition”. (See paras 8.13.1 - 8.13.5)
-  **RECOMMENDATION 109** PAGE 282
Section 77(1)(a) should be amended so that the Commissioner is required to continue endeavouring to secure a settlement only where it appears to the Commissioner that settlement is possible. (See paras 8.15.1 - 8.15.2)
-  **RECOMMENDATION 110** PAGE 283
Section 78 should be broadened to encompass all charging complaints. (See paras 8.16.1 - 8.16.3)
-  **RECOMMENDATION 111** PAGE 285
Consideration should be given to including in, or following, section 81(5) a provision that the Prime Minister may refer a report given under section 81(4) to the Intelligence and Security Committee. (See paras 8.19.4 - 8.19.6)

**RECOMMENDATION 112**

PAGE 288

Provision should be made by amending section 82(2), or otherwise, to allow Tribunal proceedings to be brought by the Proceedings Commissioner where there is a breach of an assurance given to the Privacy Commissioner under section 74 or 77. (See paras 8.20.10 - 8.20.13)

**RECOMMENDATION 113**

PAGE 290

Section 88(2) and (3) should be more closely aligned with section 88(2) - (6) of the Human Rights Act 1993. (See paras 8.26.3 - 8.26.5)

9. PROCEEDINGS OF COMMISSIONER

**RECOMMENDATION 114**

PAGE 294

Section 92 should be amended so that the Commissioner may require an agency to comply with a requirement made pursuant to section 91 within a shorter period than 20 working days where the urgency of the case so requires. (See paras 9.4.1 - 9.4.5)

**RECOMMENDATION 115**

PAGE 295

Section 92(3) should be repealed. (See paras 9.4.7 - 9.4.9)

**RECOMMENDATION 116**

PAGE 298

Section 95(3) should be amended to specify that:
(a) the Prime Minister, in respect of paragraph (a); and
(b) the Attorney-General, in respect of paragraph (b);
personally may exercise the power to prevent disclosure of information to the Privacy Commissioner. (See paras 9.7.1 - 9.7.4)

10. INFORMATION MATCHING

**RECOMMENDATION 117**

PAGE 307

The definition of “adverse action” in section 97 should be supplemented by a paragraph relating to decisions to impose a penalty and to recover a penalty earlier imposed. (See paras 10.2.7 - 10.2.9)

**RECOMMENDATION 118**

PAGE 309

Consideration should be given to amending the definitions of “authorised information matching programme” and “information matching programme” in section 97 so as to exclude manual comparison from their scope. (Refer paras 10.2.14 - 10.2.20)

**RECOMMENDATION 119**

PAGE 309

Consideration should be given to replacing references in Part X and elsewhere to “information matching” by “data matching”. (See para 10.2.21.)

**RECOMMENDATION 120**





PAGE 310

The definition of “specified agency” in section 97 should be amended so that the agencies are listed in the Third Schedule alongside the information matching provisions to which they relate. (See paras 10.2.26 - 10.2.29)

**RECOMMENDATION 121**

PAGE 312

Consideration should be given to:
(a) including in section 97, in addition to the definition of “specified agency” (which could be renamed “participating agency”), definitions of “source agency”, “matching agency” and “user agency”; and
(b) utilising these newly defined terms in Part X and the Fourth Schedule as appropriate. (See paras 10.2.30 - 10.2.34)

-  **RECOMMENDATION 122** PAGE 313
Section 98(c) should be amended so that alternative means of achieving the objective of a proposed matching programme are examined with a view to considering whether they would be more, or less, privacy intrusive. (See paras 10.3.9)
-  **RECOMMENDATION 123** PAGE 315
Section 98(e) should be amended so that in considering whether a programme involves information matching on a scale that is excessive, regard is also had to:
(iii) the amount of detail about an individual that will be disclosed as a result of the programme; and
(iv) the frequency of matching. (See paras 10.3.10 - 10.3.13)
-  **RECOMMENDATION 124** PAGE 316
Section 98(f) should be amended so that the information matching guideline refers not only to the information matching rules but also to Part X of the Act. (See paras 10.3.14 - 10.3.18)
-  **RECOMMENDATION 125** PAGE 316
Section 99 should be amended to require the parties to review any information matching agreement at least once every three years and to report the results of that review to the Privacy Commissioner. (See para 10.4.4)
-  **RECOMMENDATION 126** PAGE 319
Consideration should be given to limiting the Inland Revenue Department's exemptions in section 101(5) and information matching rule 6(3) so that IRD is exempted from obligations to destroy information only where this is an intended objective of the programme. (See paras 10.6.3 - 10.6.4)
-  **RECOMMENDATION 127** PAGE 320
Section 102 should be amended to make clear that it refers to both the 60 working day time limit in section 101(1) and the 12 month time limit in section 101(2). (Refer paras 10.7.4 - 10.7.6)
-  **RECOMMENDATION 128** PAGE 320
Section 103(1) should be amended by substituting a 10 working day period for the present 5 working day period. (See paras 10.8.1 - 10.8.2)
-  **RECOMMENDATION 129** PAGE 323
Section 103(1A) should be repealed. (See paras 10.8.3 - 10.8.6)
-  **RECOMMENDATION 130** PAGE 324
Consideration should be given to amending section 104(2)(e) to adopt aspects of the clause 12(v) of the Australian Data-matching Program (Assistance and Tax) Guidelines. (See paras 10.9.4 - 10.9.6)
-  **RECOMMENDATION 131** PAGE 325
Section 105 should be amended so that the annual information matching report may be submitted separately from the annual report required under section 24. (See paras 10.10.1 - 10.10.5)
-  **RECOMMENDATION 132** PAGE 326
Consideration should be given to funding the Privacy Commissioner's information matching monitoring activities by charges on specified agencies involved in carrying out information matching programmes. (See paras 10.10.6 - 10.10.10)

**RECOMMENDATION 133**

PAGE 329

Information matching rule 1 should be retitled “Openness and public awareness concerning operation of programme” and consideration should be given to enhancing the rule by detailing mandatory requirements, and a variety of discretionary methods, by which agencies may ensure that individuals who will be affected by a programme are made aware of its existence and effect. (See paras 10.12.5 - 10.12.9)

**RECOMMENDATION 134**

PAGE 330

Information matching rule 2 should be amended by deleting the phrase “unless their use is essential to the success of the programme” and replace it with provision for agencies to apply to the Commissioner for approval to use unique identifiers where the Commissioner is satisfied that their use is essential to the success of the programme. (See paras 10.12.10 - 10.12.16)

**RECOMMENDATION 135**

PAGE 332

A more informative heading should be given to information matching rule 5 and consideration should be given to redrafting the rule in a clearer fashion possibly drawing upon the Australian approach and using defined terms. (See paras 10.12.23 - 10.12.25)

**RECOMMENDATION 136**

PAGE 334

Information matching rule 8(2) should be repealed or, if retained, its purpose and effect made plain. (See paras 10.12.31 - 10.12.33)

**RECOMMENDATION 137**

PAGE 334

Provision should be made for terms used in Part X, and the information matching rules, to be able to be defined in the information matching rules themselves. (See paras 10.12.34 - 10.12.36)

**RECOMMENDATION 138**

PAGE 335

Section 108 should be amended to replace the reference to “subclause (2)(d)(i) of principle 2 or paragraph (e)(i) of principle 11” with a reference to all of the exceptions to principles 2 and 11. (See paras 10.13.1 - 10.13.4)

11. LAW ENFORCEMENT INFORMATION**RECOMMENDATION 139**

PAGE 345

Section 112 providing for local authorities to be authorised to have access to law enforcement information should be repealed together with the definition of “local authority” in section 110 and the references to local authorities in the Fifth Schedule. (See paras 11.2.4 - 11.2.5, 11.4.1 - 11.4.7)

**RECOMMENDATION 140**

PAGE 346

If section 112 is not repealed in its entirety then the reference to local authorities in the Fifth Schedule relating to the national register of drivers’ licences should be repealed. (See paras 11.4.8 - 11.4.10)

**RECOMMENDATION 141**

PAGE 346

All existing approvals given under section 4E of the Wanganui Computer Centre Act 1976 should be reviewed and:

- (a) any that are unnecessary should be revoked;
- (b) any which need to be continued should be replaced, within a reasonable time, with a new notice carrying appropriate conditions issued under section 112. (See paras 11.4.11 - 11.4.12)

**RECOMMENDATION 142**

PAGE 347

Provision should be made to allow the Fifth Schedule to be amended by Order in Council subject to a five year sunset clause. (See paras 11.5.1 - 11.5.7)

12. MISCELLANEOUS PROVISIONS

**RECOMMENDATION 143**

PAGE 351

Consideration should be given to the merits of making consistent amendments to:

- (a) section 115 of the Act;
- (b) section 48 of the Official Information Act 1982; and
- (c) section 41 of the Local Government Official Information and Meetings Act 1987;

to meet the perceived difficulties of interpretation raised by the distinction in the first and second subsections of each of these provisions between “the making available of information” and the “making available of, or the giving of access to, information”. (See paras 12.2.1 - 12.2.4)

**RECOMMENDATION 144**

PAGE 352

Section 96, or the First Schedule, should be amended so that the obligation of secrecy clearly extends to former Commissioners and persons formerly engaged or employed in connection with the work of the Commissioner. (See paras 12.3.3 - 12.3.5)

**RECOMMENDATION 145**

PAGE 353

Sections 117, 117A and 117B should be combined into a single consultation section with consideration given to placing the details of the officer with whom consultation is to be undertaken and the purposes of such consultation in a new schedule. (See para 12.6.2)

**RECOMMENDATION 146**

PAGE 353

Consideration should be given to making provision, along the lines of sections 117 to 117B, for consultation with other statutory bodies such as the Police Complaints Authority. (See para 12.6.3)

**RECOMMENDATION 147**

PAGE 357

Sections 124 and 125 should be repealed and replaced by a single brief provision providing that the relevant delegation provisions in the Local Government Act 1974 and Local Government Official Information and Meetings Act 1987 apply. (See paras 12.13.1 - 12.13.5)

**RECOMMENDATION 148**

PAGE 359

There should be an offence provision created concerning any person who intentionally misleads an agency by:

- (a) impersonating the individual concerned; or
- (b) misrepresenting the existence or nature of authorisation from the individual concerned;

in order to make the information available to that person or another person or to have the personal information used, altered or destroyed. (See paras 12.16.5 - 12.16.8)

**RECOMMENDATION 149**

PAGE 360

There should be an offence created of knowingly destroying documents containing personal information to which the individual concerned has sought access in order to evade an access request. (see paras 12.16.9 - 12.16.12)

**RECOMMENDATION 150**

PAGE 362

Section 107 should provide that every information for an offence must be laid within 12 months from the time when the matter of the information arose. (See paras 12.16.17 - 12.16.19)

**RECOMMENDATION 151**

PAGE 366

A provision should be included to prohibit employers, prospective employers, and providers of services, requiring individuals to exercise their access rights to obtain criminal history information as a condition of obtaining employment, continuing employment, or obtaining services. (See paras 12.18.6 - 12.18.17)

**RECOMMENDATION 152**

PAGE 367

Provision should be made to constrain contractual requirements that oblige individuals to supply copies of health records. (See paras 12.18.18 - 12.18.19)

**RECOMMENDATION 153**

PAGE 368

Section 132 should be repealed. (See paras 12.21.1 - 12.21.3)

13. SCHEDULES

**RECOMMENDATION 154**

PAGE 370

The Ministry of Justice, together with the Privacy Commissioner and the specified agencies, should study the Fourth Schedule to consider whether:

- (a) the information matching rules might be expressed more clearly;
- (b) the clarity or effectiveness of the rules would be enhanced by the use of new concepts, which might be defined, or by defining existing concepts that are used;
- (c) the use of flow-charts would improve presentation. (See para 13.5.2)

Appendix A

A

Acknowledgements

A

389

Although the responsibility for the entire report rests with me as Privacy Commissioner, in some respects it is the culmination of contributions, small and large, from literally hundreds of people. It is impossible to identify everyone who has assisted by name. However, I wish to thank a number of the significant contributors. I apologise for any omissions - with so many people having contributed in so many ways, a record of their names is not always “readily retrievable” to borrow a phrase from section 29.

I first wish to acknowledge the work of Blair Stewart, then Manager, Codes and Legislation and now Assistant Commissioner, who has been responsible to me for undertaking the review. Blair has coordinated, or undertaken, much of the work required to research the issues, to consult stakeholders, and to propose to me responses to the legislative issues uncovered. He has been closely involved with the writing of this report. All of this has been done while continuing to assist me with a full workload of legislative issues, codes of practice, and, latterly, information matching matters.

STAFF OF THE OFFICE OF THE PRIVACY COMMISSIONER

The process has been managed by Blair Stewart and the staff reporting to him. Wendy Bertram, Codes and Legislation Officer, has been a mainstay in assisting with the review processes in 1997 and 1998. Brigid Feehan, a former Codes and Legislation Officer, assisted in earlier internal phases of the review.

Other staff have contributed in a variety of ways. This commenced with a year long series of monthly “brainstorming” sessions in 1995 and continued with a variety of review sessions in late 1997.

Margaret Gibbons and Frances Ermerins have been responsible for typing the report and have had the unenviable task of handling ever-changing drafts. I have been grateful for their diligence. Gillian Rook and Sharon Newton also assisted in the processing of submissions.

PRELIMINARY INPUT

Several steps were taken before the launch of the discussion papers in mid-1997. In August 1996 I wrote to Chief Executives of government departments seeking preliminary views as to issues which ought to be examined. A similar letter was sent in October 1996 to a selection of representative bodies in the private sector. I acknowledge the assistance derived from the responses of the following agencies:

Public sector agencies

- Ministry of Justice;
- Department of Internal Affairs;
- Department of Research, Science and Technology;
- Department of Labour;
- Ministry of Consumers Affairs;

- Department for Courts;
- Ministry of Cultural Affairs;
- State Services Commission;
- Department of Corrections;
- Ministry of Youth Affairs;
- Ministry of Civil Defence;
- Solicitor-General;
- Ministry of Defence;
- Ministry of Health;
- NZ Defence Force;
- Accident Compensation and Rehabilitation Insurance Corporation;
- Transport Accident Investigation Commission.

Private sector representative bodies

- NZ Law Society;
- NZ Employers Federation;
- NZ Medical Association;
- NZ Bankers' Association;
- National Council for Women;
- Insurance Council;
- Newspapers Publishers Association.

In their personal capacities, helpful preliminary comments were also made by Grant Liddell, Dr Paul Roth and Professor Geoff Schmitt.

A questionnaire on information matching was circulated in early 1997. Completed questionnaires were helpfully received from the following:

- Ministry of Defence;
- NZ Post Electoral Enrolment Centre;
- NZ Customs Service;
- Inland Revenue Department;
- Ministry of Education;
- Department for Courts;
- Department of Corrections;
- Ministry of Justice;
- Department of Social Welfare; and
- Department of Labour.

DISCUSSION PAPERS AND CONSULTATION PROCESSES

The 12 discussion papers released from mid 1997 were a key feature of the consultation process. A number of these were prepared in-house by Blair Stewart, and, in one case, Wendy Bertram. Others were prepared on contract by legal consultants including Robert Stevens of Auckland, John Edwards of Wellington, and Janet Girvan of Christchurch. A team effort was involved in critiquing and rewriting aspects of the various papers before release.

I was pleased at the response to the discussion papers and individually list those individuals and organisations who made submissions at Appendix B. Although the extent of the submissions, compiled into four volumes, has created considerable work for me and my office I have been gratified to find so many people willing to take the time to engage in the various issues.

During November 1997 I held a series of consultation meetings in Dunedin, Christchurch, Wellington and Auckland. Although my staff organised most of these, I acknowledge the assistance of Nicola Peart and Andrew Alston, of the Faculties of Law at the University of Otago and the University of Canterbury, for setting up consultation meetings at their respective universities.

SPECIALIST CONSULTATION

I have appreciated the willingness of the Public Law Group in the Ministry of Justice to act as a soundingboard on some issues and to research answers to others, particularly those concerning passage through Parliament of the Privacy of Information Bill. I particularly acknowledge the assistance of Allison Bennett.

During December 1997 I hosted a series of closed discussion meetings corresponding with the subject matter of each of the 12 discussion papers. These small meetings primarily involved myself, my managers, legal consultants and a variety of staff. However, each meeting was broadened by the inclusion of an expert or two from outside my office. The participants from outside my office were invited in their personal capacity and not as a representative of their particular organisations. I am pleased to acknowledge the assistance of:

- Robert Buchanan, Director, Law Commission;
- Katrine Evans, Faculty of Law, Victoria University of Wellington;
- Cathie Harrison, Barrister and Solicitor.
- Brigid Feehan, NZ Law Society;
- Richard Fisher, Assistant Ombudsman;
- Sir John Robertson, former Chief Ombudsman.

Written comments were also received from Professor Geoff Schmitt.

A number of submissions were received from the local government sector which raised further issues for consideration. In December 1997 I convened a special consultation meeting touching upon issues especially relevant to local government. I was gratified that people from as far afield as Palmerston North and the Wairarapa were willing to travel to Wellington to inform me of their views. I acknowledge the assistance of Geraldine Murphy of Wellington City Council on local government issues and the participation of the following organisations in the meeting:

- Department of Internal Affairs;
- Local Government New Zealand;
- Wellington City Council;
- Palmerston North City Council;
- Porirua City Council;
- Carterton District Council;
- Hutt City Council;
- Masterton District Council;
- Upper Hutt City Council.

As I wrote my report I took the opportunity to consult with organisations which might be thought likely to be affected by some of the proposed recommendations. It is not appropriate to list them here but I do wish to say that I appreciated the comments made. I also sought comment on issues concerning the interaction of other laws with the Act and I am grateful for the written comments from, amongst others, the:

- Ombudsmen;
- Inspector-General of Intelligence and Security;
- Banking Ombudsman;
- Clerk of the House of Representatives;
- Chief Human Rights Commissioner;
- Police Complaints Authority;
- Ministry of Justice;
- Wellington City Council.

ASSISTANCE FROM OVERSEAS

My staff have been conferring with Privacy Commissioners in other jurisdictions on various technical matters relevant to the review since late-1995. Valuable published material was gathered including, in particular, reports of reviews of privacy laws in other jurisdictions. A number of Commissioners and other agencies have answered particular ques-

tions which have contributed to this report. I especially wish to acknowledge the following:

Privacy and Data Protection Commissioners and their staff

- Privacy Commissioner, Australia;
- Privacy Commissioner, Canada;
- Registratiekamer, The Netherlands;
- Commission d'accès à l'information, Quebec;
- Data Protection Registrar, United Kingdom;
- Information and Privacy Commissioner, Alberta;
- Privacy Commissioner for Personal Data, Hong Kong;
- Information and Privacy Commissioner, British Columbia;
- Information and Privacy Commissioner, Ontario;
- Berliner Datenschutzbeauftragter, Germany.

Other agencies

- Department of Justice, Canada;
- Ombudsman, Manitoba;
- Department of Justice, Nova Scotia.

MISCELLANEOUS ASSISTANCE

I have appreciated the expert assistance on some technical and legal issues received from Janice Lowe of Wellington and Robert Stevens of Auckland.

The Ministry of Justice Information Services Group and National Archives assisted by facilitating access to the files of the Information Authority and Wanganui Computer Centre Privacy Commissioner respectively.

The Parliamentary Service assisted in securing photographs of former MPs. Other photographic credits appear with the photographs themselves.

Design and Production of *'Necessary and Desirable – Privacy Act 1993 Review'* by Shane Clapson of Element Design Ltd.

Appendix B

B

List of Submissions

B
393

The following is an alphabetical list of people and organisations which made submissions on the discussion papers. Many organisations are listed here and in attributed quotations in the report as having made a submission. In some cases the submission may not be the formal position of the whole organisation but rather an expression of views of an officer, employee or division of that organisation.

Abortion Law Reform Association NZ Inc
 Age Concern Canterbury
 Anti-Bases Campaign
 Ashburton Branch, NCW
 Association for Market Research Organisations
 Association of Superannuation Funds NZ Inc
 Auckland City
 Auckland Council for Civil Liberties (Inc)
 Auckland District Council of Social Service
 Auckland Healthcare Services Ltd
 Averton, Rosamund
 Bagozzi, Daniela
 Banking Ombudsman
 Baynet CRA Ltd
 Bertram, Wendy
 Brown, Leslie
 Cairns, Joanne
 Cameron, Alan
 Campaign for Nuclear Disarmament (Wellington) Inc
 Chapple, Jim
 Commonwealth Press Union
 Comrie, Clive
 Consumers' Institute
 Crown Law Office
 Dalziel, Kathryn
 Debenham, Terry
 Department for Courts
 Department of Corrections
 Department of Internal Affairs
 Department of Internal Affairs - Local Government & Community Policy
 Department of Labour
 Dynamic Controls Ltd
 Eastbay Health
 Ellis Gould
 Family Planning Association NZ
 Federation of Women's Health Councils Aotearoa NZ

FINSEC
 Franklin District Council
 Gordon, Mary-Ellen
 Government Communications Security Bureau
 Government Superannuitants Assn of NZ (Inc)
 Hager, Nicky
 Hattaway, Peter
 Health and Disability Commissioner
 Healthcare Otago Ltd
 Human Rights Commission
 Hutt City Council
 Inland Revenue Department
 Inspector-General of Intelligence and Security
 Insurance Council of NZ Inc
 Investment Savings and Insurance Association
 Janczewski, Dr Lech
 Jorgensen, Murray
 Kaitia Council of Social Services
 Kelly, Paul
 Kensington Swan
 Kerkin, Sarah
 King, Chris
 Langdon, Kristin
 Local Government New Zealand
 MacDonald, Ian
 MacFarlane, J J D
 Makani, Tania
 Manukau City Council
 Market Research Society of NZ
 Mein, Dr J N
 Ministry of Agriculture
 Ministry of Commerce - Business and Registries Branch
 Ministry of Education
 Ministry of Fisheries
 Ministry of Justice
 Ministry of Transport
 Napier Council of Social Services
 National Council of Women
 National Library
 Northland Chamber of Commerce
 Nurse Maude Association
 Nursing Council of NZ
 NZ Airline Pilots' Association
 NZ Association of Citizens Advice Bureaux
 NZ Association of Crown Research Institutes (Inc)
 NZ Association of Parking Enforcement Authorities
 NZ Association of Social Workers Aotearoa
 NZ Bankers' Association
 NZ Business Roundtable
 NZ College of Midwives (Inc)
 NZ Council for Civil Liberties
 NZ Defence Force
 NZ Employers Federation
 NZ Federation of Family Budgeting Services (Inc)
 NZ General Practitioners' Association Inc
 NZ Law Society - Privacy Working Group
 NZ Medical Association
 NZ Railway Superannuitants' Association

NZ School Trustees Association
 NZ Security Intelligence Service
 NZ Video Dealers Association Inc
 Office of the Commissioner for Children
 Office of the Controller and Auditor-General
 Office of the Race Relations Conciliator
 Palmerston North City Council
 Parry, David
 Pateriki-Davenport, Angela
 Patients Rights Advocacy
 Paton-Simpson, Elizabeth
 Peart, Nicola
 Phillips, Alan
 Porirua City Council
 Rajasingham, Dr Lalita
 Ridley, G F
 Robinson, Trevor
 Roth, Dr Paul
 Royal NZ College of General Practitioners
 Schizophrenia Fellowship (Auckland) Inc
 Service Workers Union
 Simon, Silke
 State Services Commission
 Suggate, Richard
 Tauranga District Council
 Te Puni Kokiri
 Teeuwen, W P
 Telecom New Zealand Ltd
 The Health Alternatives for Women (Inc)
 Transit New Zealand
 Transport Accident Investigation Commission
 Tranz Rail
 Tribunal for the Catholic Church for NZ
 Tucker, Jim
 TVNZ Group
 Valuation New Zealand
 Wellington City Council
 Wellington Community Law Centre
 Wellington District Law Society - Constitutional Matters Committee
 Westpac Trust
 Westwater, Margret

B

B

395

Appendix C

Recent Overseas Privacy Legislation

C

C

397

This lists general privacy or data protection laws that have been enacted, or have come into force, during or since 1993. Sectoral laws, such as the Personal Health Information Act 1997 of Manitoba and the Australian Capital Territory Health Records (Privacy and Access) Act 1997, are generally not included. English translations are given for the titles of foreign laws.

1992

Freedom of Information and Protection of Privacy Act, British Columbia.
 Protection of Personal Data and Disclosure of Data of Public Interest Act, Hungary
 Law on the Protection of Private Life Regarding the Protection of Personal Data, Belgium
 Federal Law on Data Protection, Switzerland.

1993

An Act Respecting the Protection of Personal Information in the Private Sector, Quebec.
 Freedom of Information and Protection of Privacy Act, Nova Scotia.
 Data Protection Law, Monaco.

1994

Freedom of Information and Protection of Privacy Act, Alberta.
 Access to Information and Protection of Privacy Act, Northwest Territories.
 Law on the Protection of Personal Information in the Public Sector, Korea.

1995

Personal Data (Privacy) Ordinance, Hong Kong.
 Law on Information, Informatisation and Information Protection, Russian Federation.
 Computer Processed Personal Data Protection Law, Taiwan.

1996

Law on Protection of Individuals and Legal Persons Regarding the Processing of Personal Data, Italy.
 Data Protection Act, Estonia.
 Law on Legal Protection of Personal Data, Lithuania.
 Access to Information and Protection of Privacy Act, Yukon Territory.

1997

Freedom of Information and Protection of Privacy Act, Manitoba.
 Law on Protection of the Individual against Processing of Personal Data, Greece.
 Data Protection Act, Poland.

1998

Law on Personal Data Protection in Information Systems, Slovakia.

Protection of Personal Information Act, New Brunswick.

Data Protection Act, United Kingdom

Appendix D

Legislative Background

LEGISLATIVE INFLUENCES

1972

Preservation of Privacy Bill - private member's initiative encouraged the introduction of Labour Government's Privacy Commissioner Bill and Wanganui Computer Centre Bill in 1975.

1974

Private Investigators and Security Guards Act 1974 - perhaps the first NZ statute expressly directed to protection of privacy.

1975

Privacy Commissioner Bill - Government bill did not survive the change of government.

1976

Wanganui Computer Centre Act 1976 - established NZ's first Privacy Commissioner and directly influenced Part XI of the Privacy Act.

1977

Human Rights Commission Act 1977 - the Human Rights Commission's privacy brief was later transferred to the Privacy Commissioner.

1980

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data - influenced the Health Amendment Act 1988 and the Privacy Act itself.

Danks Committee - recommended repeal of the Official Secrets Act 1951 and proposed key features of an official information regime.

1981

Council of Europe Convention No 108 - influential European counterpart to the OECD Guidelines.

1982

Official Information Act 1982 - the part concerning access to personal information later transferred into the Privacy Act.

1983

Australian Law Reform Commission Privacy Report - influenced the Australian Privacy Act 1988 and thereby indirectly the Privacy Act.

1987

Official Information Amendment Act 1987 and *Local Government Official Information and Meetings Act 1987* - extended access rights to broader range of public sector agencies.

Data Privacy: An Options Paper - report to the Minister of Justice influenced the shape of subsequent privacy legislation.

1988

Information Authority Report on the Subject of Collection and Use of Personal Information - not generally implemented but influenced the Health Amendment Act 1988.

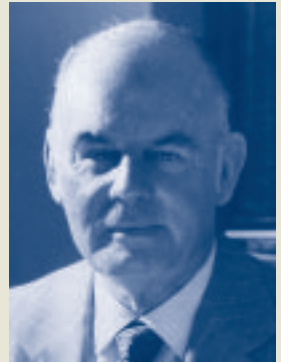
Privacy Act 1988 (Australia) - many aspects, particularly the information privacy principles, copied into the Privacy of Information Bill.

Computer Matching and Privacy Protection Act 1988 (USA) - influenced the approach to information matching in the Privacy of Information Bill.

D

D

399



Sir George Laking:
New Zealand's first Wanganui
Computer Centre Privacy
Commissioner.

PHOTO: OFFICE OF THE
OMBUDSMEN



Sir James Wicks: Wanganui
Computer Centre Privacy
Commissioner from 1978 to
1983.

PHOTO: OFFICE OF THE PRIVACY
COMMISSIONER

Health Amendment Act 1988 - first NZ law to implement the OECD collection limitation principle, also included health sector security safeguards and disclosure controls, repealed with the enactment of the Privacy Act and 1993 health restructuring.

1989

Broadcasting Act 1989 - required programme standards to be consistent with the privacy of the individual and enabled complaints to be taken to the Broadcasting Standards Authority.

1990

Data-matching Program (Assistance and Tax) Act 1990 (Australia) - directly influenced the approach taken to information matching in the Privacy Act.

Draft European Community Directive on Data Protection - rekindled worldwide interest in data protection.

1991

Information Privacy Bill - private member's initiative which illustrated bipartisan support for privacy law.

Privacy of Information Bill - following select committee study led directly to the Privacy Commissioner Act 1991 and Privacy Act 1993.

Privacy Commissioner Act 1991 - established Privacy Commissioner and information matching, later consolidated into the Privacy Act.

1992

Draft EC Directive on Data Protection - European Parliament draft highlighted trading partners' need to consider privacy laws.

LIST OF PRIVACY COMMISSIONERS

Wanganui Computer Centre Act 1976

Sir George Laking

17 February 1977 - 31 March 1978 concurrently with appointment as Chief Ombudsman.

The Honourable Justice McGechan

1 April 1978 - 28 September 1978 pending appointment of a full-time Commissioner. High Court Judge who was then Deputy Chairman of Wanganui Computer Centre Policy Committee.

Sir James Wicks

29 September 1978 - 28 September 1983. Retired Chief Stipendiary Magistrate.

P L Molineaux

29 September 1983 - 30 June 1993. Retired District Court Judge and former Director of the NZ Security Intelligence Service.

Privacy Commissioner Act 1991

B H Slane

15 April 1992 - 30 June 1993. Barrister and solicitor, former President of the NZ Law Society and Chairman of the Broadcasting Tribunal.

Privacy Act 1993

B H Slane

1 July 1993 onwards. First 5 year term commenced under the 1991 Act was continued by section 133 of the Act and followed by a 3 year reappointment.



Paul Molineaux: The longest serving, and final, Wanganui Computer Centre Privacy Commissioner. In several of his reports he emphasised the shortcomings of the 1976 legislation under which he was appointed and urged the enactment of a general information privacy statute.

PHOTO: P MOLINEAUX



Bruce Slane: Originally appointed under the Privacy Commissioner Act 1991 and the first Privacy Commissioner to serve under the Privacy Act 1993.

PHOTO: OFFICE OF THE PRIVACY COMMISSIONER

Appendix E

Parliamentary Counsel Office Drafting Style Changes

E

E

401

The Parliamentary Counsel Office adopted a series of changes in drafting style in legislation effective from 1 January 1997. The changes were set out in *A Guide to Working with the PCO*, pp 65-68. This appendix sets out six of the relevant changes, with the original notes, and relates them to the Privacy Act 1993.

Existing practice

Proposed practice

1 Dropping “of this Act” etc. to make shorter cross-references within a document, eg.

section 2 of this Act	to	section 2
subsection (1) of this section	to	subsection (1)
paragraph (a) of this subsection	to	paragraph (a)
regulation 2 of these regulations	to	regulation 2
etc.		

Notes: *Discretion should be used about dropping the extra words if this might result in uncertainty (eg. if the provision being referred to is not clear from the context). This change will apply across the board, (eg. it will also apply when a new section is being inserted into an existing Act).*

Privacy Act: The formulation “of this Act” appears at various places (see, for example, sections 1, 2, and 7) as does the phrase “of this subsection” (see, for example, sections 2(2), 3(3), and 8(1)). Within the information privacy principles the phrase “subclause (1) of this principle” appears in various places (see, for example, information privacy principles 3(2), 3(3) and 3(4)).

2 Numbering Parts in Arabic instead of Roman, eg.

Parts I, II, III, IV, etc	to	Parts 1, 2, 3, 4
---------------------------	----	------------------

Privacy Act: The twelve Parts of the Privacy Act are currently identified by Roman numerals.

3 Numbering Schedules 1, 2 instead of First, Second, etc, eg.

First Schedule	to	Schedule 1
----------------	----	------------

Note: *If referring to a First Schedule in existence before 1997, for example, continue to refer to it as the First Schedule, not Schedule 1.*

Privacy Act: The Privacy Act’s eight schedules are currently labelled First, Second, etc.

4 Alternatives for “shall” in appropriate cases, eg.

This Act shall bind the Crown	to	This Act binds the Crown
The Minister shall ensure	to	The Minister must ensure
There shall be a Commissioner called ...	to	There is a Commissioner called ...

Note: *To indicate the fact of establishment in this case consider whether the marginal note should read “Establishment of Commissioner”. Also, the definition of Commissioner could read “... means the Commissioner established by section 00”.*

The Commissioner shall be appointed by ...	to	The Commissioner is appointed
The Commissioner shall be a Crown entity	to	The Commissioner is a Crown entity
The functions of the Commissioner shall be sections 16 to 19 of this Act shall apply	to	The functions of the Commissioner are sections 16 to 19 apply
shall not	to	does not

Notes: *If the situation requires a “shall”, the word may still be used. This change will apply across the board, (eg. it will also apply when a new section is being inserted into an existing Act full of “shalls”).*

Privacy Act: Each of the above examples of the use of “shall” appear in the Privacy Act. Perhaps of particular note is the fact that each of the twelve information privacy principles uses the word “shall” at least once (two of the principles use “shall” twice, one uses “shall” four times and principle 7 uses “shall” five times).

5 Authority to drop unnecessary “except as provided”/“subject to”/ “notwithstanding” formulations if appropriate, eg.

(2) Subject to subclause	to	(2) The Guild is exempted from ...
(3) of this clause, the Guild is exempted ...		(3) The exemption granted by subclause
(2) is subject to the condition that...	to	(3) [That exemption] [<i>or, if more than one exemption, the exemption in subclause (2)</i>] is subject to the condition that ...

Privacy Act: Examples in the Privacy Act include sections 8, 6, 60 and 126.

6 Analysis

Include the text of Schedule headings in the analysis.

Privacy Act: The present analysis does not list the Act’s eight Schedules.

Appendix F

F

Reports to the Minister of Justice

F

403

Date	Subject of report
1992	
<i>July</i>	Passports Bill (disclosure of passports database to Australia)
1993	
<i>August</i>	Children, Young Persons, and Their Families Amendment Bill (mandatory reporting of suspected child abuse)
<i>August</i>	Health and Disability Commissioner Bill and Supplementary Order Paper No 247
1994	
<i>June</i>	Finance Bill (amending State Owned Enterprises Act)
<i>July</i>	Whistleblowers Protection Bill
<i>October</i>	Tax Administration Bill (the effect on individual access rights of IRD's secrecy provision)
<i>October</i>	Law Reform (Miscellaneous Provisions) (No 3) Bill (amendments to the Private Investigators and Security Guards Act)
<i>November</i>	Copyright Bill (privacy of certain photographs and films)
1995	
<i>January</i>	Local Government Law Reform Bill (registration of dogs)
<i>January</i>	Domestic Violence Bill
<i>February</i>	Parliamentary Privilege Bill
<i>February</i>	Medical Practitioners Bill
<i>February</i>	Criminal Investigations (Blood Samples) Bill (taking of blood samples for DNA analysis from suspects and establishment of DNA profile databank)
<i>April</i>	Medical Practitioners Bill (supplementary comments)
<i>May</i>	Financial Transactions Reporting Bill (moneylaundering)
<i>May</i>	Residential Tenancies Amendment Bill
<i>May</i>	Social Welfare Reform Bill and Supplementary Order Paper No. 84 (giving effect to recommendations of inquiry into privilege provisions of section 11 Social Security Act)
<i>July</i>	Radio New Zealand Bill (Privacy Act amendment in privatisation paving legislation)
<i>July</i>	Courts and Criminal Procedure (Miscellaneous Provisions) Bill (publication of names of fines defaulters)
<i>October</i>	Electoral Reform Bill (information matching of electoral and immigration information)*

<i>November</i>	Legal framework surrounding Ministerial release of personal details in matters of public controversy
<i>November</i>	Paperwork Reduction Bill
1996	
<i>January</i>	Law Reform (Miscellaneous Provisions) (No 5) Bill (amending the Privacy Act)
<i>February</i>	Intelligence and Security Agencies Bill
<i>April</i>	Tax Reduction and Social Policy Bill (information matching between ACC and IRD)*
<i>April</i>	Tax Reduction and Social Policy Bill (information matching between NZISS and NZES)*
<i>July</i>	Adoption Amendment Bill (No 2)
<i>July</i>	Proposed information matching programme between Department for Courts and Department Social Welfare*
1997	
<i>January</i>	Harassment and criminal associations
<i>April</i>	Trans-Tasman Mutual Recognition Bill and transborder data flows
<i>April</i>	Harassment and Criminal Associations Bill (interception of private communications)
<i>April</i>	Electoral Act 1993
<i>April</i>	Social Security Amendment Bill
<i>May</i>	Protected Disclosures Bill
<i>June</i>	Postal Services Bill
<i>August</i>	Amendment to Section 126A Social Security Act (information matching between Department for Courts and DSW)*
<i>August</i>	Taxation (Remedial Provisions) Bill (tax file numbers)
<i>September</i>	Telephone analysers and call data warrants
<i>November</i>	Witness Anonymity Bill
<i>November</i>	Disclosure of executive remuneration under the Companies Act
<i>December</i>	Interpretation Bill
1998	
<i>January</i>	Inaccuracy of list of overstayers (Electoral Act information match)
<i>January</i>	Radiocommunications Amendment Bill
<i>January</i>	Health Occupational Registration Amendment Bill
<i>March</i>	Land Transport Bill: Photo ID Driver Licences
<i>March</i>	Proposed information matching programme between the Department for Courts and IRD*
<i>August</i>	Broadcasting Amendment Bill (No 2) (Codes of broadcasting standards)

**These reports concerned section 13(1)(f) examinations of proposed information matching provisions.*

Appendix G

G

Commissioner's Functions Under Other Statutes

G

405

The Privacy Commissioner's functions are principally set out in section 13 of the Privacy Act. Section 13(1)(u) provides that these include such other functions and duties as are conferred or imposed on the Commissioner by or under "this Act *or any other* enactment." The provision allows for a flexible, and evolving, set of functions. Those conferred to date are set out below in the following six categories:

- complaint mechanisms;
- Commissioner's approval;
- consultations;
- appointment to another body;
- codes of practice;
- information matching.

COMPLAINTS MECHANISMS

Health Act 1956

- complaints concerning a health agency's failure or refusal to transfer health records (section 22F).

Domestic Violence Act 1995

- complaints concerning a registrar's refusal to suppress residential details on a public register relating to an individual who fears for his or her personal safety if those details were to be released (sections 118-120 of the Act and clause 11 of the Domestic Violence (Public Register) Regulations 1996).

Social Security Act 1964

- complaints concerning a breach of the code of conduct applying to obtaining information under section 11 of the Social Security Act (section 11B);
- complaints concerning failure by the Director General of Social Welfare to comply with section 131C of the Social Security Act which requires certain notice to be given before reducing benefits for failure of a work-test (section 131F).

Adoption (Intercountry) Act 1997

- implicitly authorises complaints, normally barred by section 34 of the Privacy Act, concerning certain access requests by non-New Zealanders subject to intercountry adoption orders (section 13).

COMMISSIONER'S APPROVAL

Passports Act 1992

- requires the Commissioner's approval in relation to agreements for the supply of the New Zealand passport database to Australia (section 36);
- requires the Commissioner's approval in relation to agreements to the supply of the passport database to the NZ Customs Service (section 35).

CONSULTATIONS

Official Information Act 1982

- requires the Ombudsmen to consult in relation to review of official information access requests where privacy is a possible ground for withholding information (section 29B).

Local Government Official Information and Meetings Act 1987

- requires the Ombudsmen to consult in relation to review of local government official information access requests where privacy is a possible ground for withholding information (section 29A).

Health and Disability Commissioner Act 1994

- requires the Health and Disability Commissioner to consult in relation to the preparation of a draft Code of Health and Disability Services Consumers' Rights (sections 19 and 23);
- requires the Health and Disability Commissioner to consult in respect of any review of the Code of Health and Disability Services Consumers' Rights (sections 21 and 23);
- requires the Health and Disability Commissioner to consult in relation to the appropriate means of dealing with a complaint which is more properly within the jurisdiction of the Commissioner (section 40).

Customs and Excise Act 1996

- requires the chief executive of the New Zealand Customs Service to consult in relation to agreements for disclosure of information to overseas law enforcement and customs agencies (section 281).

Financial Transactions Reporting Act 1996

- requires the Commissioner of Police to consult in relation to the preparation of suspicious transaction reporting guidelines (section 25).

Social Security Act 1964

- requires the Director-General of Social Welfare to consult on the issue or amendment of a code of conduct applying to obtaining information under section 11 of the Social Security Act (section 11B).

Ombudsmen Act 1975

- requires the Ombudsmen to consult in relation to the appropriate means to deal with a complaint which is more properly within the jurisdiction of the Commissioner (section 17A).

Inspector General of Intelligence and Security Act 1996

- allows the Inspector-General to consult in relation to any of the Inspector-General's functions (section 12).

APPOINTMENT TO OTHER BODIES

Human Rights Act 1993

- designates the Commissioner as a Human Rights Commissioner (section 7).

CODES OF PRACTICE

Local Government Act 1974

- confers additional powers to specify search references, in relation to the register of charges, by code of practice (section 122ZI).

Dog Control Act 1996

- confers additional powers in relation to the making of codes of practice affecting dog registers (section 35).

Domestic Violence Act 1995

- confers additional powers in relation to the making of codes of practice to prescribe aspects of the regime governing non-publication of information relating to protected persons on public registers (sections 122 to 124).

INFORMATION MATCHING

Social Security Act 1964

- authorises the Commissioner to monitor compliance with certain requirements of a match between the Departments of Labour and Social Welfare as if section 103 of the Privacy Act applied (section 131G);
- provides for the monitoring of the obtaining of information from employers, and its comparison with departmental records, as if the activity were an authorised information matching programme (section 11A).

Education Act 1989

- empowers the Commissioner to settle the form in which enrolment information is disclosed by education institutions to DSW (section 226A);
- empowers the Commissioner to settle the form in which enrolment information is disclosed by private training institutions to DSW (section 238B).

G

G

407

Appendix H

Tables of Equivalent Provisions

H

H

409

Some sections in the Privacy Act were modelled on sections in the Official Information Act 1982, Ombudsmen Act 1975 or Human Rights Commission Act 1977. Following the enactment of the Privacy Act similar provisions have been included in the Human Rights Act 1993 and the Health and Disability Commissioner Act 1994. The following tables identify the corresponding provisions. Where no equivalent provision exists a (-) is used. The local Government Official Information and Meetings Act 1987 is abbreviated to LGOIMA.

RIGHTS OF ACCESS AND CORRECTION		
Privacy Act	Official Information Act	LGOIMA
ipp6(1)	s.24	s.23
ipp6(1)(a)	–	–
ipp6(1)(b)	s.24(1)	s.23(1)
ipp6(2)	s.24(3A)	s.23(3)
ipp6(3)	–	–
ipp7(1)(a)	s.26(1)(a)	s.25(1)(a)
ipp7(1)(b)	s.26(1)(b)	s.25(1)(b)
ipp7(2)	–	–
ipp7(3)	–	–
ipp7(4)	–	–
ipp7(5)	s.26(2)	s.25(2)

SAVINGS		
Privacy Act	Official Information Act	LGOIMA
s.7(1)	s.52(3)(a)	s.44(2)(a)
s.7(2)(a)	s.52(3)(b)(i)	s.44(2)(b)(i)
s.7(2)(b)	s.52(3)(b)(ii)	s.44(2)(b)(ii)
s.7(3)(a)	s.52(3)(b)	s.44(2)(b)
s.7(3)(b)(i)	s.52(3)(b)(i)	s.44(2)(b)(i)
s.7(3)(b)(ii)	s.52(3)(b)(ii)	s.44(2)(b)(ii)
s.7(4)	–	–
s.7(5)	–	–
s.7(6)	–	–

REASONS FOR REFUSING ACCESS TO INFORMATION		
Privacy Act	Official Information Act	LGOIMA
s.27(1)(a)	ss.6(a), 27(1)(a)	–
s.27(1)(b)	ss.6(b), 27(1)(a)	–
s.27(1)(c)	ss.6(c), 27(1)(a)	ss.6(a), 26(1)(a)
s.27(1)(d)	ss.6(d), 27(1)(a)	ss.6(b), 26(1)(a)
s.27(2)(a)	ss.7(a), 27(1)(a)	–
s.27(2)(b)	ss.7(b), 27(1)(a)	–
s.27(2)(c)	ss.7(c), 27(1)(a)	–
s.28(1)(a)	ss.9(2)(b)(i), 27(1)(a)	ss.7(2)(b)(i), 26(1)(a)
s.28(1)(b)	ss.9(2)(b)(ii), 27(1)(a)	ss.7(2)(b)(ii), 26(1)(a)
s.28(2)	s.9(1)	s.7(1)
s.29(1)(a)	s.27(1)(b)	s.26(1)(b)
s.29(1)(b)	s.27(1)(c)	s.26(1)(c)
s.29(1)(c)	s.27(1)(d)(repealed)	s.26(1)(d)(repealed)
s.29(1)(d)	s.27(1)(e)(repealed)	s.26(1)(e)(repealed)
s.29(1)(e)	s.27(1)(f)(i)(repealed)	s.26(1)(f)(repealed)
s.29(1)(f)	s.27(1)(g)	s.26(1)(g)
s.29(1)(g)	cf.s.9(2)(ba)(i)	cf.s.7(2)(c)
s.29(1)(h)	–	–
s.29(1)(i)	s.18(c)(ii), cf.s.52(1)	s.17(c)(ii), cf.s.44(1)
s.29(1)(j)	s.27(1)(h)	s.26(1)(h)
s.29(2)(a)	cf.ss.18(f), 24(1)(b)	cf.ss.17(f), 23(1)(b)
s.29(2)(b)	s.18(e)	s.17(e)
s.29(2)(c)	s.18(g)	s.17(g)
s.29(3)	s.27(2)	s.26(3)
s.30	s.27(1A)	s.26(2)
s.31	s.27A(repealed)	–
s.32	s.10	s.8

PROCEDURAL PROVISIONS RELATING TO ACCESS TO AND CORRECTION OF INFORMATION		
Privacy Act	Official Information Act	LGOIMA
s.33	–	–
s.34	cf.s.24(2)	cf.s.23(1A)
s.35(1)	cf.s.15(1A)	cf.s.13(1A)
s.35(2)	–	–
s.35(3)	cf.s.15(1A)	cf.s.13(1A)
s.35(4)	–	–
s.35(5)	s.15(2)	s.13(3)
s.35(6)	–	–
s.36	–	–
s.37	s.12(3)	s.10(3)
s.38	s.13	s.11
s.39	s.14	s.12
s.40(1)	s.15(1)	s.13(1)
s.40(2)	s.15(3)	s.13(4)
s.40(3)	s.15(4)	s.13(5)
s.40(4)	s.15(5)	s.13(6)
s.41	s.15A	s.14
s.42	s.16	s.15
s.43	s.17	s.16
s.44	s.19	s.18
s.45	s.25	s.24

H

H

411

COMPLAINTS AND INVESTIGATIONS			
Privacy Act	Ombudsmen Act	Human Rights Act	Health and Disability Commissioner Act
s.67	–	cf.ss.13, 75	s.31
s.68	s.16	–	s.32
s.69	cf.s.13	s.75	s.35
s.70	cf.s.17(3)	cf.s.76(3)	s.36
s.71	cf.s.17	s.76	s.37
s.72	s.17A	–	s.40
s.73	s.18(1)	s.78	s.41
s.74	–	s.81	cf.s.42
s.75	s.24	s.79	s.43
s.76	–	s.80	cf.s.61
s.77	cf.s.22	cf.ss.81, 82	s.45
s.78	–	–	–
s.79	–	–	–
s.80	s.18(6)	–	s.48
s.81	–	–	–
s.82	–	s.83	s.50
s.83	–	s.83(4)	s.51
s.84	–	s.86(1)	s.52
s.85	–	s.86	s.54
s.86	–	s.84	s.55
s.87	–	s.85	s.56
s.88	–	s.88	s.57
s.89	–	–	s.58

PROCEEDINGS			
Privacy Act	Ombudsmen Act	Official Information Act	LGOIMA
s.90	cf.s.18(2), (3), (7)	–	–
s.91	cf.s.19(1), (2), (8)	–	–
s.92(1)	–	ss.29A(1), 35(1A)	ss.29(1), 38(2)
s.92(2)	–	ss.29A(1), 35(1A)	ss.29(1), 38(2)
s.92(3)	–	ss.29A(6), 35(1A)	ss.29(1), 38(2)
s.93(1)	–	ss.29A(2), 35(1A)	ss.29(2), 38(2)
s.93(2)	–	ss.29A(3), 35(1A)	ss.29(3), 38(2)
s.93(3)	–	ss.29A(4), 35(1A)	ss.29(4), 38(2)
s.93(4)	–	ss.29A(5), 35(1A)	ss.29(5), 38(2)
s.94(1)	s.19(5)	–	–
s.94(1A)	s.19(5A)	–	–
s.94(1B)	s.19(5B)	–	–
s.94(2)	s.19(7)	–	–
s.95(1)	s.19(3)	–	–
s.95(2)	s.19(4)	–	–
s.95(3)	s.20(1)	–	–
s.96	s.26	–	–

MISCELLANEOUS PROVISIONS			
Privacy Act	Ombudsmen Act	Official Information Act	LGOIMA
s.115	–	s.48	s.41
s.116	s.21	–	–
s.117	s.21A	cf.s.29B	cf.s.29A
s.118	–	–	–
s.119	–	s.11	s.9
s.120	–	ss.30(3), 35(6)	ss.30(2), 38(6)
s.121	s.28	–	–
s.122	s.28(6)	–	–
s.123	s.28(3), (4)	–	–
s.124	–	–	s.42
s.125	–	–	s.43
s.126	–	–	–
s.127	s.30	–	–
s.128(a)	–	s.47(c)	–
s.128(b)	–	s.47(e)	s.55(c)

Appendix I

I

LIST OF PUBLIC REGISTERS		
Enactment	Section	Description of Register
Deeds Registration Act 1908	21,22	Book of primary entry
	30	Record book copies
Industrial and Provident Societies Act 1908	3D	General register authority (see SR 1952/221)
Incorporated Societies Act 1908	33	Register of incorporated societies
Industrial and Provident Societies Amendment Act 1952	20	Register of charges (Registrar)
	26	Register of charges (Society)
Land Transfer Act 1952	33	Register of grants and titles
	50	Provisional registration
Marriage Act 1955	7	List of marriage celebrants
Insolvency Act 1967	118	Bankrupts' discharge and undischarged bankrupts
Local Government Act 1974	122ZH, ZI	Register of local authority charges
Local Election and Polls Act 1976	7B	Electoral roll
	7BA	Residents electoral roll
	7BB	Ratepayers electoral roll
	7BC	Rolls for divided local government areas
	7BD	Rolls where 1 or more communities
Friendly Societies and Credit Unions Act 1982	5	Registrar's register of rules etc
	40	Society's register of members etc
	130	Credit union's register of members etc
Transport (Vehicle and Driver Registration and Licensing) Act 1986	18	Register of motor vehicles
	45	National register of drivers licences
Rating Powers Act 1988	113	Rate records
Motor Vehicles Securities Act 1989	5	Register of security interests
Building Act 1991	27	Territorial authority records (building consents, project information memoranda, building WOFs etc)
	53	Register of building certifiers
Te Ture Whenua Maori Act 1993	263	Maori incorporation share registers
Companies Act 1993	87, 88	Share registers
	189	Company records
	360	Registers of companies, overseas companies
Electoral Act 1993	100	Corrupt practices list
	101, 103, 104, 105, 106, 107	Electoral rolls
	108	Habitation indexes
	109	Dormant file
	211, 212	Candidate returns
Births Deaths and Marriages Registration Act 1995	5, 7(2), 8	Births registers
	24, 25	Adoptions registers
	34, 36, 48(3), 50	Deaths registers
	53, 56, 58	Marriage registers
Dog Control Act 1996	34	Dogs register
Fisheries Act 1996	98, 124	Fishing vessel and permit registers
Rating Valuations Act 1998	7	District valuation rolls

Appendix J

Complaints Graphs

J

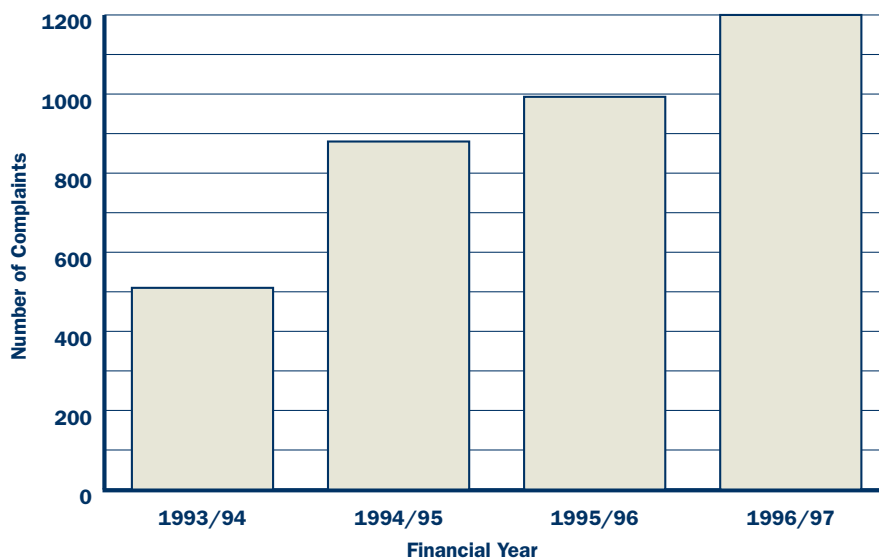
J

415

The graphs presented here illustrate the complaints made to the Privacy Commissioner. They also show the resources available to process complaints and illustrate the growing complaints queue. The graphs have been chosen to illustrate general trends. Further specific figures may be obtained from annual reports. The Commissioner's financial and reporting year is 1 July to the 30 June the following year and complete series of figures exist for 1993/94 through to 1996/97. It has sometimes been possible to display figures through to 31 December 1997 or the end of March 1998.

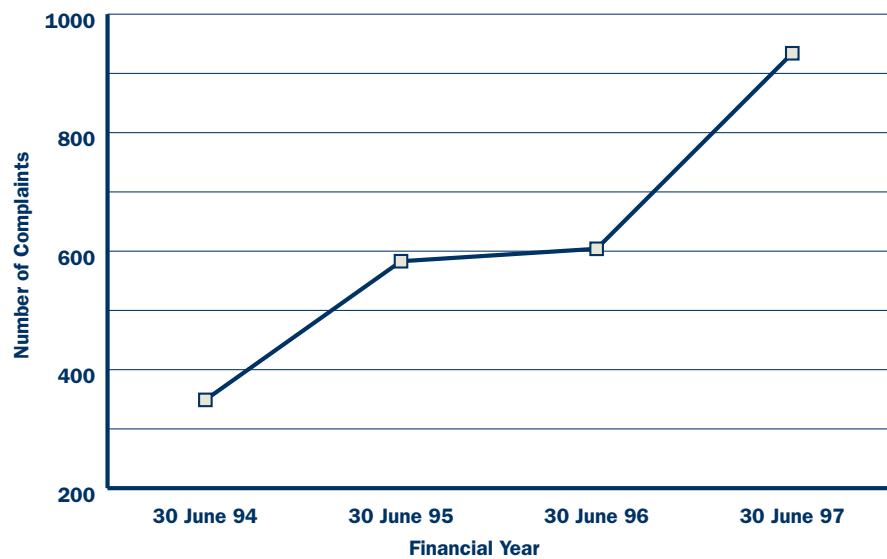
A: INCOMING COMPLAINTS

Figure J1: Complaints received



This illustrates the growth of complaints since the jurisdiction commenced on 1 July 1993. At some point the jurisdiction will mature and complaints plateau off.

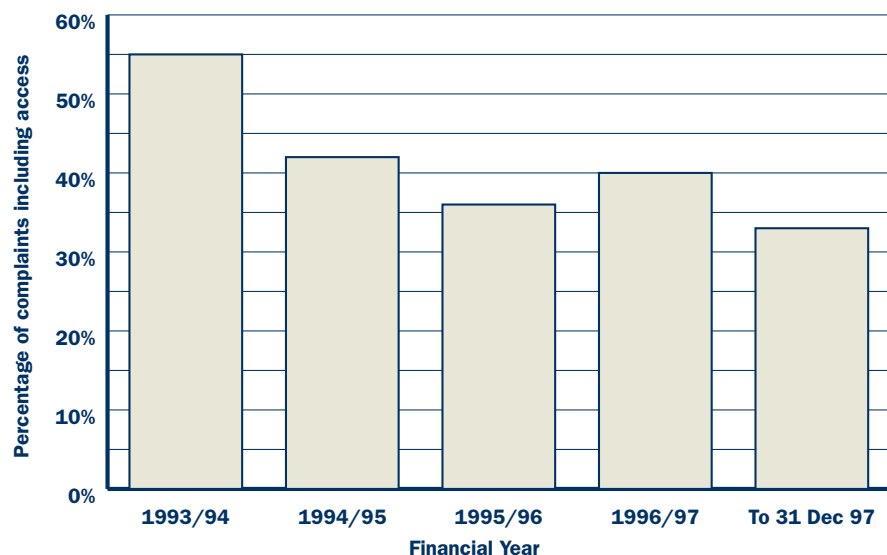
Figure J2: Complaints carried forward at year end



The number of complaints on hand comprised the total of new complaints received *and* those carried forward from the previous year. The number of complaints carried forward has continued to grow because of the number of new complaints outstripping the number of complaints closed (see graph J3).

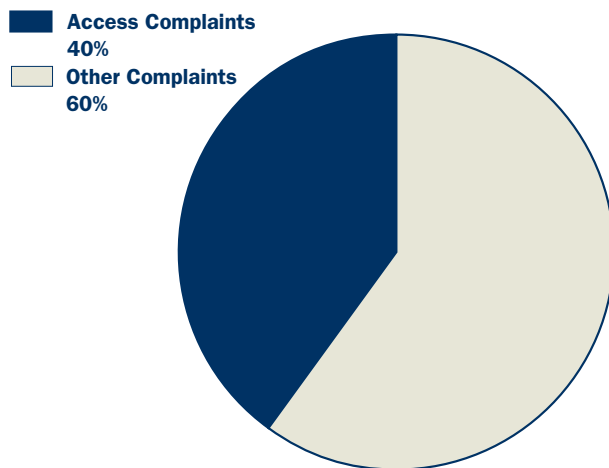
B: NATURE OF COMPLAINTS

Figure J3: Complaints which include access as a percentage of total annual complaints



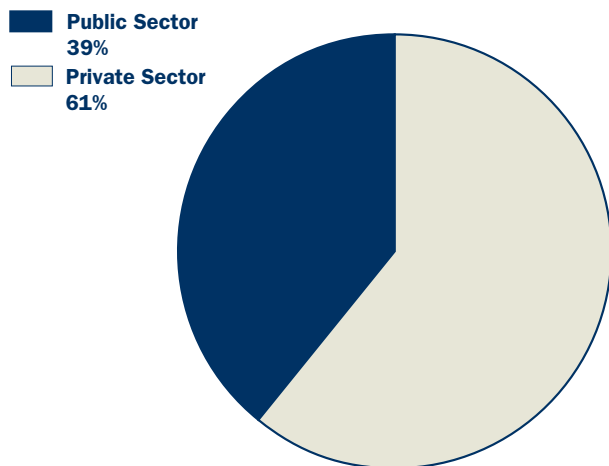
The single largest category of complaints are those concerning access to personal information. Access rights existed in the public sector and were transferred into the Privacy Act. From the start this part of the jurisdiction was “up and running”. Access complaints have become a smaller percentage of total complaints in later years as people become more familiar with other entitlements under the Act. This and the following graph illustrate complaints which include access as an issue – some of the same complaints also included other issues such as accuracy or disclosure.

Figure J4: Ratio of complaints which include access to other complaints



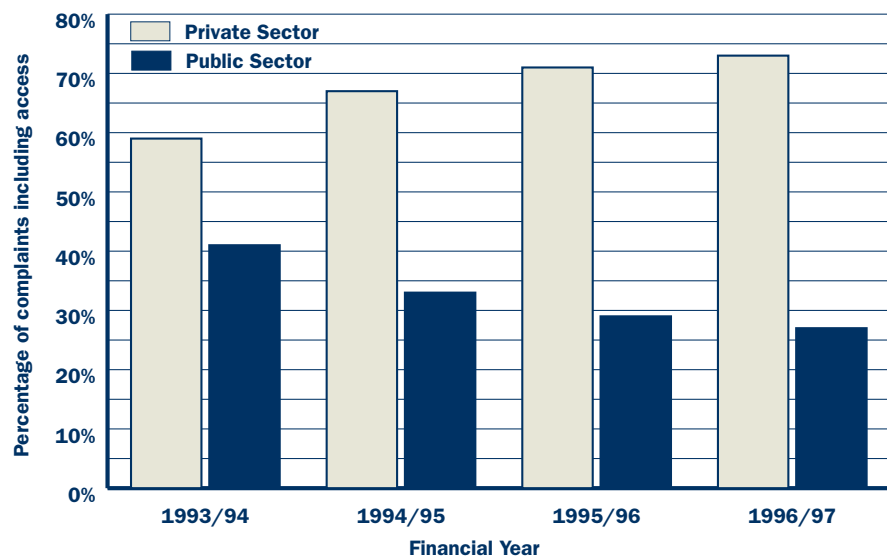
All complaints received to 30 June 1997 have been totalled to present this figure.

Figure J5: Public/private sector breakdown of complaints



Complaints received to 31 December 1997 have been totalled for this graph. Complaints may be made against agencies regardless of whether they are in the public or private sectors. However, complaints received are coded as to which sector is relevant. These figures should be taken as a general indication only given the difficulty of coding in some cases and certain broad categorisations adopted by the office (for example, all education-related complaints are categorised as public sector notwithstanding that this is not always the case).

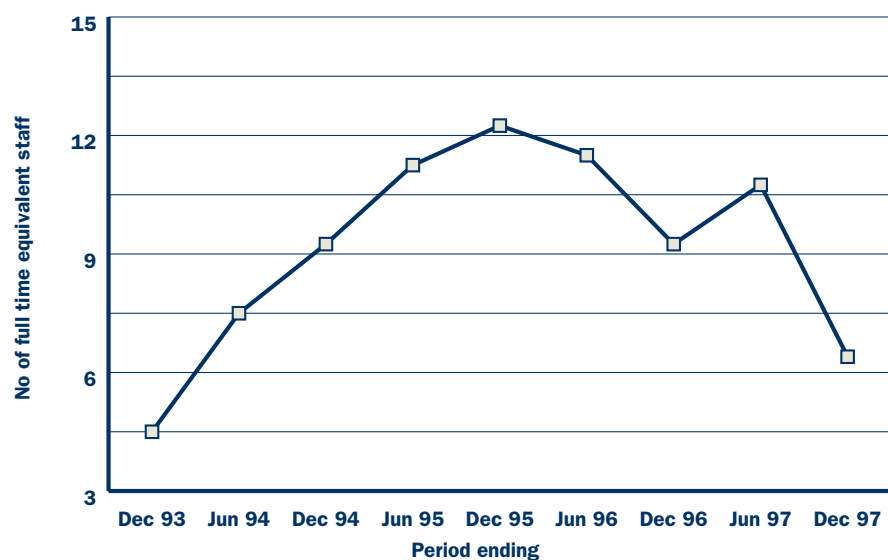
Figure J6: Complaints which include disclosure by sector



Complaints which include disclosure are the largest category after access complaints. This graph shows the proportion of complaints lodged against public and private sector agencies which concern disclosure. An increasing proportion of the disclosure complaints received by the office have concerned private sector agencies.

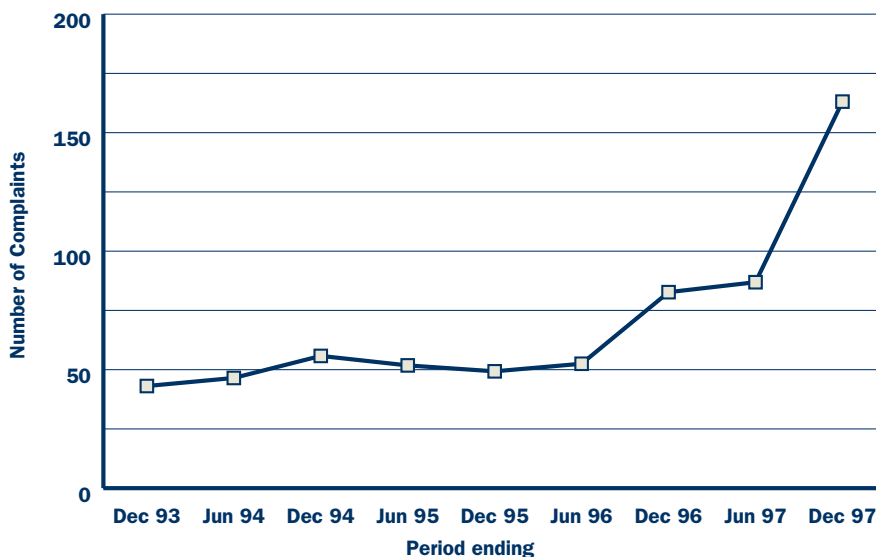
C: RESOURCES DEPLOYED AND COMPLAINTS QUEUE

Figure J7: Number of investigators



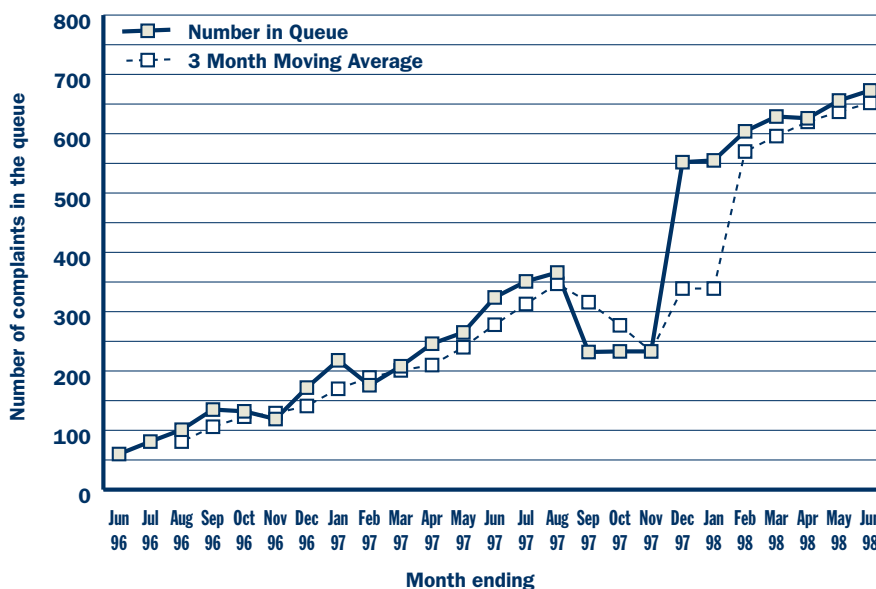
This graph shows the number of investigation personnel for the four years from December 1993. The number of full time equivalent positions is presented since the office uses part-time employees and contractors to supplement full time personnel. The figures also take account of extended staff absences. The graph begins six months after the commencement of the complaints jurisdiction and shows the numbers building to the end of 1995. With the office beginning to mature, staff departures began to feature. Staff were not always immediately replaced, and in later years, sometimes not replaced at all, due to funding difficulties. The apparent dramatic fall in the final months of 1997 is explained by the coincidence of staff departures, a staff member taking maternity leave, and two staff taking 3 months professional legal studies at the same time (the latter two returning in mid-December).

Figure J8: Complaints on hand per investigator



This graph should be read together with the graph showing the incoming complaints (figure J1), and the number of investigation personnel (figure J7). The trend is plain. Until June 1996 the increasing investigation personnel kept up with the increasing number of complaints. The position has deteriorated since and has manifested itself in the complaints queue (see figure J9). That the final leap in complaints on-hand per investigator in the final six months was partly reversed in the immediately following period (not shown) when staff on legal professional studies returned to work. The graph does not illustrate complaints actually allocated to Investigators – each Investigator is given a manageable allocation with the balance held in the queue.

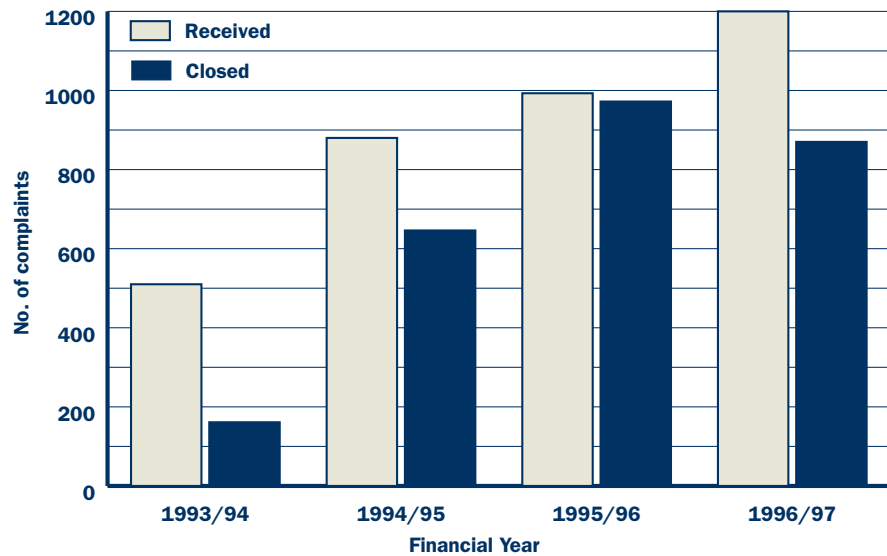
Figure J9: Complaints queue



A complaints queue was instituted in 1996. This graph shows the queue as a trend with the contributing factors, the complaints received and closed, presented on a monthly basis. The drop in late 1997 is partly explained by the employment, on a short-term contract basis, of an experienced investigator to address certain files and a staff project to close old files. As can be seen, without the availability of on-going investigation personnel available, the previous trend has reasserted itself in 1998.

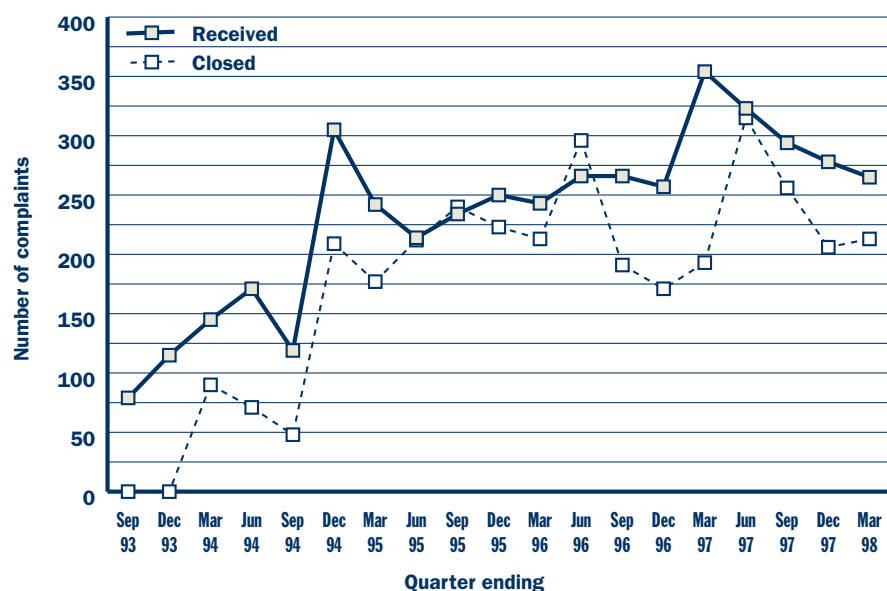
D. CLOSURE AND COMPLAINT OUTCOMES

Figure J10: Complaints received/closed on annual basis



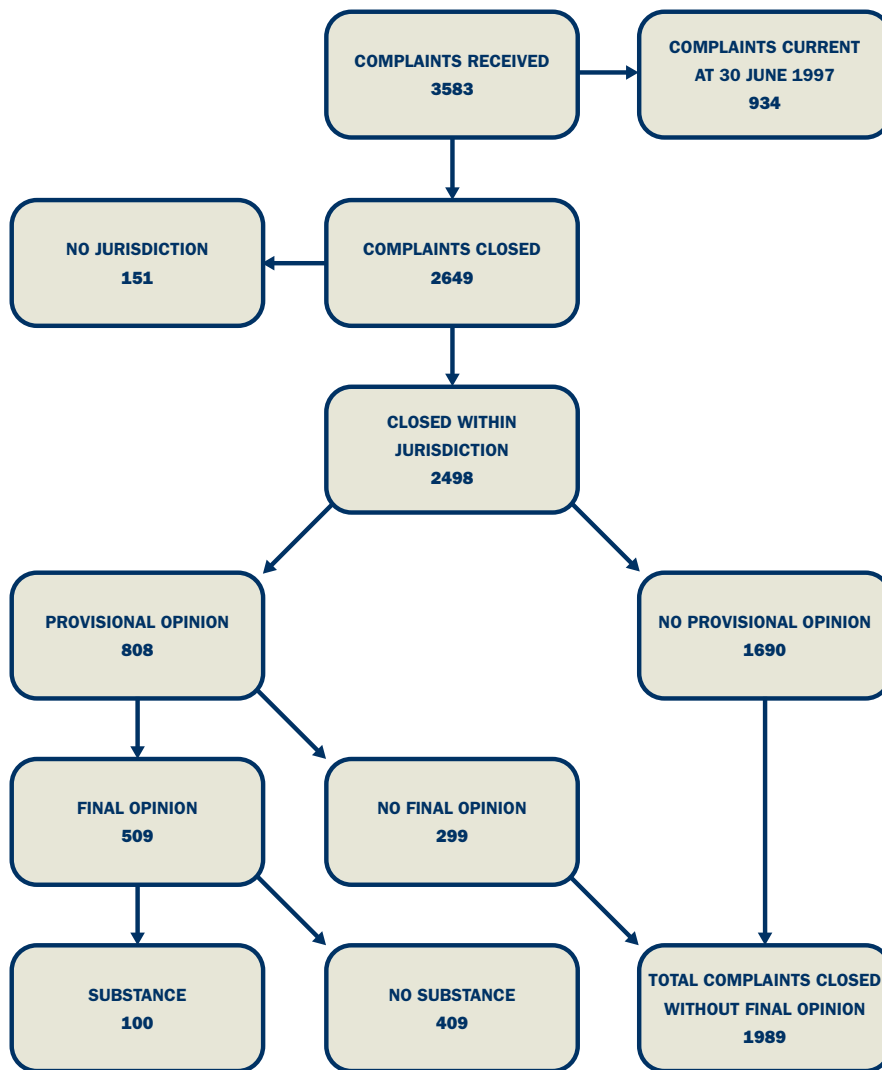
This gives the “big picture” on a yearly basis as to the volume of incoming complaints and the office’s performance in dealing with them. As already noted, the number of complaints has continued to rise. It has never been possible to close complaints files to meet the rate of incoming complaints although this was most nearly achieved in 1995/96. The significant feature is the difference between the number of complaints received and those closed. This difference is passed on to the following year and constitutes an increasing backlog.

Figure J11: Complaints received/closed on quarterly basis



This graph shows more detail than the previous graph. The figures are presented on a quarterly basis and illustrate the nine months since the close of the 1996/97 year. Since July 1996 there has never been a quarter in which fewer than 250 complaints have been received.

Figure J12: Analysis of complaints received to 30 June 1997



This graph shows the status of the 3583 complaints received in the first 4 years as at the end of the 1996/97 year.

