



Telecommunications (Interception and Access) Act 1979

No. 114, 1979

Compilation No. 117

Compilation date:	2 April 2022
Includes amendments up to:	Act No. 31, 2022
Registered:	26 April 2022

Prepared by the Office of Parliamentary Counsel, Canberra

About this compilation

This compilation

This is a compilation of the *Telecommunications (Interception and Access) Act 1979* that shows the text of the law as amended and in force on 2 April 2022 (the *compilation date*).

The notes at the end of this compilation (the *endnotes*) include information about amending laws and the amendment history of provisions of the compiled law.

Uncommenced amendments

The effect of uncommenced amendments is not shown in the text of the compiled law. Any uncommenced amendments affecting the law are accessible on the Legislation Register (www.legislation.gov.au). The details of amendments made up to, but not commenced at, the compilation date are underlined in the endnotes. For more information on any uncommenced amendments, see the series page on the Legislation Register for the compiled law.

Application, saving and transitional provisions for provisions and amendments

If the operation of a provision or amendment of the compiled law is affected by an application, saving or transitional provision that is not included in this compilation, details are included in the endnotes.

Editorial changes

For more information about any editorial changes made in this compilation, see the endnotes.

Modifications

If the compiled law is modified by another law, the compiled law operates as modified but the modification does not amend the text of the law. Accordingly, this compilation does not show the text of the compiled law as modified. For more information on any modifications, see the series page on the Legislation Register for the compiled law.

Self-repealing provisions

If a provision of the compiled law has been repealed in accordance with a provision of the law, details are included in the endnotes.

Contents

Chapter 1—Introduction	1
Part 1-1—Preliminary	1
1 Short title	1
2 Commencement	1
4 Act binds the Crown	1
4A Application of the <i>Criminal Code</i>	1
4B Application to Norfolk Island	2
Part 1-2—Interpretation	3
5 Interpretation	3
5AA Eligible Commonwealth authority declarations	50
5AB Authorised officers	51
5AC Authorisation of certifying officers	51
5AD Authorisation of certifying person	53
5AE Authorisation of members of the staff of a Commonwealth Royal Commission	54
5A Communicating etc. certain information	54
5B Exempt proceedings	54
5C Information or question relevant to inspection by Ombudsman	58
5D Serious offences	59
5E Serious contraventions	66
5F When a communication is passing over a telecommunications system	67
5G The intended recipient of a communication	67
5H When a communication is accessible to the intended recipient	68
6 Interception of a communication	68
6AAA When a computer network is appropriately used by an employee etc. of a Commonwealth agency etc.	71
6AA Accessing a stored communication	72
6A Investigation of an offence	72
6B Involvement in an offence	73
6C Issue of warrant to agency or eligible authority	73
6D Judges	73
6DA Nominated AAT members	74
6DB Issuing authorities	75

6DC	Part 4-1 issuing authorities	76
6E	Lawfully intercepted information	77
6EA	Interception warrant information	77
6EAA	Preservation notice information	78
6EB	Stored communications warrant information	78
6F	Offences	79
6G	Officer of the Commonwealth, of a State or of a Territory	79
6H	Person to whom application relates	80
6J	Proceeding by way of a prosecution for an offence	81
6K	Proceeding for confiscation or forfeiture or for pecuniary penalty	81
6L	Relevant proceeding	81
6M	Terminating the appointment of an officer	85
6N	Declaration of staff members of State Police Forces	85
6P	Identification of service	85
6Q	Identification of telecommunications device	85
6R	Communications Access Co-ordinator	86
6S	Permitted purposes—integrity purposes	86
6T	When a Part 5.3 supervisory order is taken to be in force	88
6U	Succeeding Part 5.3 supervisory orders	88

Chapter 2—Interception of telecommunications 90

Part 2-1—Prohibition on interception of telecommunications 90

7	Telecommunications not to be intercepted	90
---	--	----

Part 2-2—Warrants authorising the Organisation to intercept telecommunications 95

9	Issue of telecommunications service warrants by Attorney-General	95
9A	Issue of named person warrants by Attorney-General	96
9B	Provisions applying to warrants issued under section 9 or 9A	99
10	Issue of warrant by Director-General of Security in emergency for Organisation to intercept telecommunications	100
11A	Telecommunications service warrant for collection of foreign intelligence	101
11B	Named person warrant for collection of foreign intelligence	103
11C	Foreign communications warrant for collection of foreign intelligence	105
11D	Provisions applying to foreign intelligence warrants	109

12	Persons authorised to intercept communications for Organisation	111
13	Discontinuance of interception before expiration of warrant	111
14	Certain records retained by Organisation to be destroyed	112
15	How warrants etc. to be dealt with	112
16	Additional requirements for named person warrants	115
17	Reports to be made to Attorney-General on results of interception	116
18	Evidentiary certificates	116
Part 2-3—Emergency requests authorising officers of a carrier to intercept telecommunications		119
30	Emergency requests	119
Part 2-4—Authorisation of interception for developing and testing interception capabilities		121
31	Applications for authorisation	121
31A	Attorney-General may authorise interception for developing and testing interception capabilities	122
31AA	Carrier to be notified of authorisation etc.	123
31B	Authorisation of employees of a security authority	124
31C	Destruction of records	124
31D	Reports to the Attorney-General	124
31E	Employees of security authorities	125
Part 2-5—Warrants authorising agencies to intercept telecommunications		126
Division 2—Declaration of State Law Enforcement Authorities as Agencies		126
34	Declaration of an eligible authority of a State as an agency	126
35	Preconditions for declaration	126
36	State laws requiring copies of documents to be given to responsible Minister	129
37	Revocation of declaration	129
38	Effect of revocation	130
38A	Agencies authorised to apply for Part 5.3 warrants	130
Division 3—Applications for warrants		133
39	Agency may apply for warrant	133
40	Form of application	134
41	Contents of application	135

42	Affidavit to accompany written application	135
43	Information to be given on telephone application.....	136
44	Giving further information to Judge	137
44A	Application by interception agency of Victoria	137
45	Application by interception agency of Queensland	138
45A	State law not affected	139
Division 4—Warrants		140
46	Issue of telecommunications service warrant	140
46A	Issue of named person warrant	147
47	Limit on authority conferred by warrant.....	155
48	Issue of warrant for entry on premises.....	155
49	Form and content of warrant.....	157
50	Issue of warrant on telephone application	159
51	Action by agency after warrant issued on telephone application	160
52	Judge or nominated AAT member may revoke warrant where section 51 contravened.....	160
54	Entry into force of warrants	161
55	Exercise of authority conferred by warrant.....	161
57	Revocation of warrant by chief officer	163
58	Discontinuance of interceptions under certain warrants	163
59	When revocation of certain warrants takes effect	164
59A	Notification to Secretary of the Department	164
59B	Notification to Ombudsman by Commonwealth agencies in relation to Part 5.3 warrants.....	165
60	Notification to authorised representative of carrier of issue or revocation of certain warrants	165
61	Evidentiary certificates	167
61A	Certified copy of warrant.....	169
Part 2-6—Dealing with intercepted information etc.		170
62	Application of Part	170
63	No dealing in intercepted information or interception warrant information	170
63AA	Dealing in interception warrant information for the purposes of Part 2-2, 2-5, 2-7 or 2-8.....	171
63AB	Dealing in general computer access intercept information etc.	171
63AC	Dealing in ASIO computer access intercept information etc.	173
63AD	Dealing in data disruption intercept information etc.....	176

63AE	Dealing in network activity warrant intercept information etc.....	179
63A	Dealing in connection with existing proceeding.....	181
63B	Dealing in information by employees of carriers.....	182
63C	Dealing in information for network protection purposes etc.	184
63D	Dealing in information for disciplinary purposes	184
63E	Responsible person for a computer network may communicate information to an agency.....	185
64	Dealing in connection with Organisation's or Inspector-General's functions.....	186
65	Dealing in information obtained by Organisation.....	187
65A	Employee of carrier may communicate information to agency.....	189
66	Interceptor may communicate to officer who applied for warrant or authorised person	190
67	Dealing for permitted purposes	190
68	Chief officer may communicate information obtained by agency.....	192
68A	Communicating information obtained by the Secretary of the Attorney-General's Department	198
69	State authority may ask not to receive information under section 68.....	198
70	Communicating information obtained by interception under Part 2-3	199
71	Dealing with information where interception suspected to be unlawful.....	199
72	Making record for purpose of permitted communication	200
73	Further dealing by recipient of certain information	200
74	Giving information in evidence in exempt proceeding.....	201
75	Giving information in evidence where defect in connection with warrant.....	201
75A	Evidence that has been given in exempt proceeding	202
76	Giving information in evidence in criminal proceedings under this Act	202
76A	Giving information in evidence in civil proceedings for remedial relief.....	203
77	Intercepted material and interception warrant information inadmissible except as provided	203
78	Where evidence otherwise inadmissible	204
79	Destruction of restricted records that are not likely to be required for a permitted purpose.....	205

79AA	Destruction of restricted records—information obtained before a Part 5.3 supervisory order came into force	205
79A	Responsible person for a computer network must ensure restricted records are destroyed	206
Part 2-7—Keeping and inspection of interception records		208
80	Commonwealth agencies to keep documents connected with issue of warrants	208
81	Other records to be kept by Commonwealth agencies in connection with interceptions	208
81AA	Organisation to record particulars in relation to eligible authorities of a State	210
81A	General Register of Warrants	211
81B	Regular submission of General Register to Minister	212
81C	Special Register of Warrants	212
81D	Regular submission of Special Register to Minister	215
81E	Provision of information by eligible authorities	215
83	Inspections	216
84	Reports	217
85	Ombudsman may report on other breaches of this Act	217
85A	Annual report may cover notified breaches in relation to Part 5.3 warrants	218
86	Ombudsman’s general powers	218
87	Power to obtain relevant information	219
88	Ombudsman to be given information and access notwithstanding other laws	220
89	Dealing with information for the purposes of inspection and report	221
90	Ombudsman not to be sued	222
91	Delegation by Ombudsman	222
92	Application of Ombudsman Act	223
92A	Exchange of information between Ombudsman and State inspecting authorities	223
Part 2-8—Reports about interceptions under Parts 2-3 and 2-5		225
Division 1—Reports to the Minister		225
93	Annual reports to Minister about interceptions under Part 2-3	225
94	Annual reports regarding applications and warrants under Part 2-5	225
94A	Reports regarding emergency interception action	226
94B	Reports regarding named person warrants	227

95	Minister may seek further information from Commonwealth agency.....	228
96	Annual reports by State authorities.....	228
97	Reports by Managing Directors about acts done in connection with certain warrants under Part 2-5	229
Division 2—Reports by the Minister		230
99	Annual report by Minister about warrants under Part 2-5	230
100	Report to set out how many applications made and warrants issued.....	230
101	Report to contain particulars about duration of warrants	233
102	Report to contain information about effectiveness of warrants	235
102A	Report regarding interceptions without warrant	238
102B	Report regarding international requests	238
103	Other information to be included in report	238
103A	Annual report for 1999-2000	240
103B	Deferral of inclusion of information in report	240
Division 3—Provisions about annual reports		243
104	Annual reports	243
Part 2-9—Offences		244
105	Contravention of section 7 or 63	244
106	Obstruction	244
107	Offences relating to inspections under Part 2-7	245
Part 2-10—Civil remedies		246
107A	Civil remedies—unlawful interception or communication.....	246
107B	Limitation periods etc.....	249
107C	No limitation on other liability	249
107D	Concurrent operation of State and Territory laws.....	250
107E	State or Territory courts—jurisdictional limits.....	250
107F	Extended meaning of <i>conviction</i> —orders under section 19B of the <i>Crimes Act 1914</i>	250
Chapter 3—Preserving and accessing stored communications		251
Part 3-1A—Preserving stored communications		251
Division 1—Outline of this Part		251
107G	Outline of this Part.....	251

Division 2—Domestic preservation notices	253
107H Domestic preservation notices	253
107J Conditions for giving domestic preservation notices	253
107K When a domestic preservation notice is in force	255
107L Revoking a domestic preservation notice	255
107M Persons who act on the issuing agency’s behalf	256
Division 3—Foreign preservation notices	258
107N When a foreign preservation notice can be given	258
107P Condition for giving a foreign preservation notice	258
107Q When a foreign preservation notice is in force	259
107R Revoking a foreign preservation notice	260
107S Persons who act on the AFP’s behalf	261
Division 4—Provisions relating to preservation notices	262
107T Evidentiary certificates relating to actions by carriers	262
107U Evidentiary certificates relating to actions by issuing agencies	262
107V Certified copies of preservation notices.....	263
107W How notices are to be given to carriers.....	263
Part 3-1—Prohibition on access to stored communications	264
108 Stored communications not to be accessed.....	264
Part 3-2—Access by the Organisation to stored communications	268
109 Access to stored communications under Part 2-2 warrants.....	268
Part 3-3—Access by criminal law-enforcement agencies to stored communications	269
Division 1—Applications for warrants	269
110 Criminal law-enforcement agencies may apply for stored communications warrants	269
110A Meaning of <i>criminal law-enforcement agency</i>	269
110B Declarations in relation to the Immigration and Border Protection Department.....	273
111 Form of applications.....	274
112 Contents of written applications	274
113 Affidavits to accompany written applications	274
114 Information to be given on telephone applications	275
115 Giving further information to Judge	275

Division 2—Issuing of warrants	276
116 Issuing of stored communications warrants.....	276
117 What stored communications warrants authorise	278
118 Form and content of stored communications warrants	278
119 Duration of stored communications warrants	279
Division 3—How warrants etc. are dealt with	280
120 Stored communications warrants issued on telephone applications.....	280
121 What happens when stored communications warrants are issued.....	281
122 Revocation of stored communications warrants by chief officers.....	281
123 What happens when stored communications warrants are revoked	282
124 Access to additional telecommunications services under stored communications warrants	282
Division 4—Provisions relating to execution of warrants	284
125 Entry into force of stored communications warrants	284
126 Limit on authority conferred by warrant.....	284
127 Exercise of authority conferred by warrant.....	284
128 Provision of technical assistance	285
129 Evidentiary certificates relating to actions by carriers.....	285
130 Evidentiary certificates relating to actions by criminal law-enforcement agencies	286
131 Certified copies of stored communications warrants	287
132 Obstruction	287
Part 3-4—Dealing with accessed information etc.	288
Division 1—Prohibition on dealing with accessed information etc.	288
133 No dealing with accessed information etc.	288
Division 2—Permitted dealings with accessed information	289
134 Dealing in preservation notice information or stored communications warrant information	289
135 Dealing in information by employees of carriers.....	289
136 Dealing in connection with Organisation’s functions.....	291
137 Dealing in information obtained by Organisation.....	292
138 Employee of carrier may communicate information to criminal law-enforcement agency.....	293

139	Dealing for purposes of investigation etc.	293
139A	Dealing for integrity purposes	296
139B	Dealing for purposes relating to Part 5.3 orders	296
140	Dealing with information if access suspected to be unlawful	297
141	Making record for purpose of permitted communication	298
142	Further dealing by recipient of certain information	298
142A	Communicating information obtained as a result of an international assistance application	298
143	Giving information in evidence in exempt proceeding.....	299
144	Giving information in evidence if communication unlawfully accessed.....	299
145	Evidence that has been given in exempt proceeding	300
146	Giving information in evidence in civil proceedings for remedial relief.....	300
Division 3—Admissibility of evidence		301
147	Accessed material inadmissible except as provided	301
148	Stored communications warrant information inadmissible except as provided	301
149	Evidence that is otherwise inadmissible	302
Division 4—Destruction of records		303
150	Destruction of records	303
Part 3-5—Keeping and inspection of records		304
Division 1—Obligation to keep records		304
151	Obligation to keep records.....	304
Division 3—Inspection of preservation notice records by Inspector-General of Intelligence and Security		306
158A	Functions of the Inspector-General of Intelligence and Security.....	306
Part 3-6—Reports about access to stored communications		307
Division 1—Reports to the Minister		307
159	Annual reports regarding applications and warrants under Part 3-3	307
160	Minister may seek further information from Commonwealth agency.....	307
Division 2—Reports by the Minister		308
161	Annual report by Minister about stored communications warrants	308

161A	Report to contain information about preservation notices	308
162	Report to set out how many applications made and warrants issued.....	308
163	Report to contain information about effectiveness of warrants	310
163A	Report regarding international requests	310
Division 3—Provisions about annual reports		311
164	Annual reports	311
Part 3-7—Civil remedies		312
165	Civil remedies—unlawful access or communication.....	312
166	Limitation periods etc.....	315
167	No limitation on other liability	315
168	Concurrent operation of State and Territory laws.....	316
169	State or Territory courts—jurisdictional limits	316
170	Extended meaning of <i>conviction</i> —orders under section 19B of the <i>Crimes Act 1914</i>	316
Chapter 4—Access to telecommunications data		317
Part 4-1—Permitted access to telecommunications data		317
Division 1—Outline of Part		317
171	Outline of Part	317
Division 2—General provisions		318
172	No disclosure of the contents or substance of a communication	318
173	Effect of Divisions 3 to 5.....	318
Division 3—The Organisation		319
174	Voluntary disclosure.....	319
175	Authorisations for access to existing information or documents.....	319
176	Authorisations for access to prospective information or documents.....	320
Division 4—Enforcement agencies		322
176A	Meaning of <i>enforcement agency</i>	322
177	Voluntary disclosure.....	324
178	Authorisations for access to existing information or documents—enforcement of the criminal law	325
178A	Authorisations for access to existing information or documents—locating missing persons.....	326

179	Authorisations for access to existing information or documents—enforcement of a law imposing a pecuniary penalty or protection of the public revenue	326
180	Authorisations for access to prospective information or documents.....	327
Division 4A—Foreign law enforcement		329
Subdivision A—Primary disclosures		329
180A	Authorisations for access to existing information or documents—enforcing foreign or international laws.....	329
180B	Authorisations for access to prospective information or documents—enforcing international laws	330
Subdivision B—Secondary disclosures		332
180C	Authorisations to disclose information or documents—enforcing foreign or international laws.....	332
180D	Authorisations to disclose information or documents—enforcement of the criminal law	333
Subdivision C—Conditions of disclosure to foreign law enforcement agencies		334
180E	Disclosing information etc. to foreign countries or foreign law enforcement agencies.....	334
Division 4B—Privacy to be considered when making authorisations		335
180F	Authorised officers to consider privacy.....	335
Division 4C—Journalist information warrants		336
Subdivision A—The requirement for journalist information warrants		336
180G	The Organisation	336
180H	Enforcement agencies.....	336
Subdivision B—Issuing journalist information warrants to the Organisation		337
180J	Requesting a journalist information warrant.....	337
180K	Further information	338
180L	Issuing a journalist information warrant.....	338
180M	Issuing a journalist information warrant in an emergency	339
180N	Duration of a journalist information warrant	341
180P	Discontinuance of authorisations before expiry of a journalist information warrant	342

Subdivision C—Issuing journalist information warrants to enforcement agencies	342
180Q Enforcement agency may apply for a journalist information warrant.....	342
180R Further information	343
180S Oaths and affirmations.....	343
180T Issuing a journalist information warrant	343
180U Form and content of a journalist information warrant	345
180V Entry into force of a journalist information warrant	345
180W Revocation of a journalist information warrant by chief officer	345
Subdivision D—Miscellaneous	346
180X Public Interest Advocates	346
Division 5—Uses of telecommunications data connected with provision of access	347
181 Uses of telecommunications data connected with provision of access	347
Division 6—Disclosure/use offences	348
181A Disclosure/use offences: authorisations under Division 3	348
181B Disclosure/use offences: certain authorisations under Division 4	350
182 Secondary disclosure/use offence: disclosures under Division 4	352
182A Disclosure/use offences: journalist information warrants	355
182B Permitted disclosure or use: journalist information warrants	356
Part 4-2—Procedural requirements relating to authorisations	357
183 Form of authorisations and notifications	357
184 Notification of authorisations or revocations.....	357
185 Retention of authorisations.....	358
185A Evidentiary certificates relating to acts by carriers	359
185B Evidentiary certificates relating to acts by the Organisation.....	360
185C Evidentiary certificates relating to acts by enforcement agencies	360
185D Notification etc. of authorisations intended to identify media sources.....	361
185E Reports on access to retained data	363
186 Report to Minister.....	364
186A Obligation to keep records.....	367

Chapter 4A—Oversight by the Commonwealth

Ombudsman	371
186B Inspection of records	371
186C Power to obtain relevant information	372
186D Ombudsman to be given information and access despite other laws	373
186E Application of Ombudsman Act	374
186F Exchange of information between Ombudsman and State inspecting authorities	375
186G Delegation by Ombudsman	376
186H Ombudsman not to be sued	376
186J Reports	376

Chapter 5—Co-operation with agencies 378

Part 5-1—Definitions	378
187 Definitions	378

Part 5-1A—Data retention 379

Division 1—Obligation to keep information and documents 379

187A Service providers must keep certain information and documents	379
187AA Information to be kept	382
187B Certain service providers not covered by this Part	385
187BA Ensuring the confidentiality of information	386
187C Period for keeping information and documents	386

Division 2—Data retention implementation plans 388

187D Effect of data retention implementation plans	388
187E Applying for approval of data retention implementation plans	388
187F Approval of data retention implementation plans	389
187G Consultation with agencies and the ACMA	390
187H When data retention implementation plans are in force	392
187J Amending data retention implementation plans	392

Division 3—Exemptions 394

187K The Communications Access Co-ordinator may grant exemptions or variations	394
187KA Review of exemption or variation decisions	396

Division 4—Miscellaneous	398
187KB Commonwealth may make a grant of financial assistance to service providers.....	398
187L Confidentiality of applications	398
187LA Application of the <i>Privacy Act 1988</i>	399
187M Pecuniary penalties and infringement notices.....	399
187N Review of operation of this Part	399
187P Annual reports	400
Part 5-2—Delivery points	402
188 Delivery points	402
Part 5-3—Interception capability	405
Division 1—Obligations	405
189 Minister may make determinations.....	405
190 Obligations of persons covered by a determination.....	406
191 Obligations of persons not covered by a determination in relation to a kind of telecommunications service.....	406
Division 2—Exemptions	408
192 The Communications Access Co-ordinator may grant exemptions	408
193 ACMA may grant exemptions for trial services	409
Part 5-4—Interception capability plans	410
195 Nature of an interception capability plan.....	410
196 Time for giving IC plans by carriers.....	411
197 Time for giving IC plans by nominated carriage service providers.....	411
198 Consideration of IC plans	412
199 Commencement of IC plans	414
200 Compliance with IC plans	415
201 Consequences of changed business plans	415
202 Confidential treatment of IC plans.....	415
Part 5-4A—Requirement arising from proposed changes	417
202A Purpose of Part	417
202B Carrier or provider to notify of proposed change	417
202C Communications Access Co-ordinator may notify agencies	419

Part 5-5—Delivery capability	420
203 Communications Access Co-ordinator may make determinations	420
204 Obligations of persons covered by a determination	421
205 Obligations of persons not covered by a determination in relation to a kind of telecommunications service	421
Part 5-6—Allocation of costs	422
Division 1—Outline of Part	422
206 Outline of Part	422
Division 2—Interception capability	423
207 Costs to be borne by the carriers	423
Division 3—Delivery capability	424
208 Costs to be borne by the interception agencies	424
209 Working out costs of delivery capabilities	424
210 Examination of lower cost options	426
211 ACMA may require independent audit of costs	426
Chapter 6—Miscellaneous	428
Part 6-1—Miscellaneous	428
298 Protection of persons—control order declared to be void	428
299 Dealing with information obtained under a warrant—control order declared to be void	428
299A Schedule 1	429
300 Regulations	430
Schedule 1—International production orders	431
Part 1—Introduction	431
1 Simplified outline of this Schedule	431
2 Definitions	432
3 Designated international agreement	443
3A Disallowance of regulations relating to designated international agreements	447
3B Statutory requirements certificate—designated international agreements	448
3C Australia’s treaty-making process	450
4 Message application service	451
5 Voice call application service	451

6	Video call application service.....	452
7	Storage/back-up service.....	452
8	General electronic content service.....	453
9	When material is posted on a general electronic content service.....	453
10	Uploaded material	454
10A	When a prescribed communications provider is based in, or operates in, a foreign country	454
11	Intended recipient of a communication.....	455
12	Use of a thing	455
13	Identification of a particular person.....	455
14	Eligible judge	456
15	Nominated AAT member	456
16	Issuing authority.....	457
17	Nominated AAT Security Division member	458
17A	Urgent circumstances	459
18	Meaning of expressions in other provisions of this Act.....	460
19	Extra-territorial application	460
20	Constitutional basis of this Schedule	461
Part 2—International production orders relating to the enforcement of the criminal law		462
Division 1—Introduction		462
21	Simplified outline of this Part.....	462
Division 2—International production orders relating to interception: enforcement of the criminal law		464
Subdivision A—Applications		464
22	Application for international production order—enforcement of the criminal law.....	464
23	Form of application	465
24	Contents of application.....	466
25	Affidavits to accompany written application.....	466
26	Information to be given on telephone application.....	467
27	Giving further information to eligible Judge or nominated AAT member.....	468
28	Application by interception agency of Victoria.....	468
29	Application by interception agency of Queensland	469
Subdivision B—International production orders relating to interception		471

30	Issue of international production order—enforcement of the criminal law	471
31	Content of international production order.....	478
32	Issue of further international production order	480
Division 3—International production orders relating to stored communications: enforcement of the criminal law		482
Subdivision A—Applications		482
33	Application for international production order—enforcement of the criminal law	482
34	Form of application	483
35	Contents of written application.....	483
36	Affidavits to accompany written application	483
37	Information to be given on telephone application.....	484
38	Giving further information to issuing authority	484
Subdivision B—International production orders relating to stored communications		484
39	Issue of international production order—enforcement of the criminal law	484
40	Content of international production order.....	489
41	Issue of further international production order	490
Division 4—International production orders relating to telecommunications data: enforcement of the criminal law		491
Subdivision A—Applications		491
42	Application for international production order—enforcement of the criminal law	491
43	Form of application	491
44	Contents of written application.....	492
45	Affidavits to accompany written application	492
46	Information to be given on telephone application.....	492
47	Giving further information to issuing authority	493
Subdivision B—International production orders relating to telecommunications data		493
48	Issue of international production order—enforcement of the criminal law	493
49	Content of international production order.....	496
50	Issue of further international production order	498

Part 3—International production orders relating to Part 5.3 supervisory orders	499
Division 1—Introduction	499
51 Simplified outline of this Part.....	499
Division 2—International production orders relating to interception: Part 5.3 supervisory orders	500
Subdivision A—Applications	500
52 Application for international production order—Part 5.3 supervisory order.....	500
53 Form of application	501
54 Contents of application.....	501
55 Affidavits to accompany written application.....	501
56 Information to be given on telephone application.....	502
57 Giving further information to eligible Judge or nominated AAT member.....	503
58 Application by Part 5.3 IPO agency of Victoria	503
59 Application by Part 5.3 IPO agency of Queensland	504
Subdivision B—International production orders relating to interception	506
60 Issue of international production order—Part 5.3 supervisory order	506
61 Content of international production order.....	515
62 Issue of further international production order	517
Division 3—International production orders relating to stored communications: Part 5.3 supervisory orders	519
Subdivision A—Applications	519
63 Application for international production order—Part 5.3 supervisory order.....	519
64 Form of application	520
65 Contents of written application.....	520
66 Affidavits to accompany written application.....	520
67 Information to be given on telephone application.....	521
68 Giving further information to issuing authority.....	521
Subdivision B—International production orders relating to stored communications	521
69 Issue of international production order—Part 5.3 supervisory order	521
70 Content of international production order.....	526

71	Issue of further international production order	527
Division 4—International production orders relating to telecommunications data: Part 5.3 supervisory orders		529
Subdivision A—Applications		529
72	Application for international production order—Part 5.3 supervisory order	529
73	Form of application	529
74	Contents of written application.....	530
75	Affidavits to accompany written application	530
76	Information to be given on telephone application.....	530
77	Giving further information to issuing authority	531
Subdivision B—International production orders relating to telecommunications data		531
78	Issue of international production order—Part 5.3 supervisory order	531
79	Content of international production order.....	535
80	Issue of further international production order	536
Division 5—Notification to Ombudsman by Part 5.3 IPO agencies in relation to international production orders		537
81	Notification to Ombudsman by Part 5.3 IPO agencies in relation to international production orders.....	537
Part 4—International production orders relating to national security		538
Division 1—Introduction		538
82	Simplified outline of this Part.....	538
Division 2—International production orders relating to interception: national security		539
Subdivision A—Applications		539
83	Application for international production order—national security	539
84	Form of application	542
85	Contents of application.....	542
86	Affidavits to accompany written application	543
87	Information to be given on telephone application.....	544

88	Giving further information to nominated AAT Security Division member	544
Subdivision B—International production orders relating to interception		545
89	Issue of international production order—national security	545
90	Content of international production order	551
91	Issue of further international production order	553
Division 3—International production orders relating to stored communications: national security		555
Subdivision A—Applications		555
92	Application for international production order—national security	555
93	Form of application	557
94	Contents of written application	557
95	Affidavits to accompany written application	558
96	Information to be given on telephone application	558
97	Giving further information to nominated AAT Security Division member	558
Subdivision B—International production orders relating to stored communications		559
98	Issue of international production order—national security	559
99	Content of international production order	563
100	Issue of further international production order	564
Division 4—International production orders relating to telecommunications data: national security		565
Subdivision A—Applications		565
101	Application for international production order—national security	565
102	Form of application	565
103	Contents of written application	566
104	Affidavits to accompany written application	566
105	Information to be given on telephone application	566
106	Giving further information to nominated AAT Security Division member	567
Subdivision B—International production orders relating to telecommunications data		567
107	Issue of international production order—national security	567
108	Content of international production order	570

109	Issue of further international production order	571
Part 5—Giving of international production orders		572
110	Simplified outline of this Part.....	572
111	Giving of international production orders—relevant agency.....	572
112	Giving of international production orders—the Organisation	574
Part 6—Revocation of international production orders		577
113	Simplified outline of this Part.....	577
114	Revocation of international production orders—relevant agency.....	577
115	Giving of instrument of revocation—relevant agency.....	578
116	Revocation of international production orders—the Organisation	579
117	Giving of instrument of revocation—the Organisation.....	579
118	Delegation by the chief officer of a relevant agency	580
119	Delegation by the Director-General of Security	581
Part 7—Objections to, and cancellation of, international production orders		582
120	Simplified outline of this Part.....	582
121	Prescribed communications provider may object to international production order	582
122	Cancellation of international production orders.....	583
Part 8—Compliance with international production orders		585
123	Simplified outline of this Part.....	585
124	Compliance with international production orders.....	585
125	When a prescribed communications provider meets the enforcement threshold	585
126	Civil penalty provision—enforcement.....	587
Part 9—Reporting and record-keeping requirements		588
Division 1—Introduction		588
127	Simplified outline of this Part.....	588
Division 2—Reporting requirements		589
128	Annual reports by relevant agencies.....	589
129	Reports to be made to the Attorney-General by the Director-General of Security	590
130	Annual reports by the Australian Designated Authority	591
131	Annual reports by the Minister	593

132	Deferral of inclusion of information in Ministerial report	593
Division 3—Record-keeping requirements		598
133	Keeping documents associated with international production orders—relevant agencies.....	598
134	Other records to be kept—relevant agencies	599
135	Keeping documents associated with international production orders—the Organisation.....	601
136	Other records to be kept—the Organisation	602
137	Keeping documents associated with international production orders—Australian Designated Authority	604
138	Other records to be kept—Australian Designated Authority	605
Division 4—Register of international production orders		609
139	Register of international production orders	609
Division 5—Destruction of records		611
140	Destruction of records	611
Part 10—Oversight by the Commonwealth Ombudsman		614
141	Simplified outline of this Part.....	614
142	Inspection of records—relevant agency.....	614
143	Inspection of records—Australian Designated Authority	615
144	Power to obtain relevant information	616
145	Ombudsman to be given information and access despite other laws	618
146	Application of Ombudsman Act	619
147	Exchange of information between Ombudsman and State/Territory inspecting authorities.....	620
148	Delegation by Ombudsman	620
149	Ombudsman not to be sued	621
150	Reports	621
Part 11—Disclosure of protected information		623
151	Simplified outline of this Part.....	623
152	Prohibition on use, recording or disclosure of protected information or its admission in evidence	623
153	Exceptions—general.....	623
154	Exception—disclosure to the Minister.....	627
155	Exception—disclosure to the Attorney-General.....	627
156	Exception—statistical information	628
157	Exceptions—international production orders relating to interception.....	628

158	Exceptions—international production orders relating to stored communications	636
159	Exceptions—telecommunications data	637
Part 12—Evidentiary certificates		638
160	Simplified outline of this Part	638
161	Evidentiary certificates—compliance with international production orders by prescribed communications providers	639
162	Evidentiary certificates—voluntary provision of associated information by prescribed communications providers	640
163	Evidentiary certificates—interception	647
164	Evidentiary certificates—stored communications	649
165	Evidentiary certificates—telecommunications data	650
166	Evidentiary certificates—Australian Designated Authority	651
Part 13—Incoming orders and requests		653
167	Simplified outline of this Part	653
168	Incoming orders and requests—exemptions from various prohibitions	653
169	Interaction with the <i>Privacy Act 1988</i>	654
Part 14—Miscellaneous		656
170	Simplified outline of this Part	656
171	Electronic service of documents	656
172	International production order issued in response to a telephone application—action required	657
173	Duty of nominated AAT Security Division member	659
174	Certified copy of international production order—interception agency	659
175	Certified copy of international production order—criminal law-enforcement agency	660
176	Certified copy of international production order—enforcement agency	660
177	Certified copy of international production order—Part 5.3 IPO agency	660
178	Certified copy of international production order—the Organisation	662
179	Delegation by the Australian Designated Authority	663
180	Minor defects in connection with international production order	663
181	Protection of persons—control order declared to be void	664
182	Specification of international agreements	664

183	Operation of the <i>Mutual Assistance in Criminal Matters Act 1987</i> not limited.....	665
184	Other functions or powers not limited	665

Endnotes	666
Endnote 1—About the endnotes	666
Endnote 2—Abbreviation key	668
Endnote 3—Legislation history	669
Endnote 4—Amendment history	688

An Act to prohibit the interception of, and other access to, telecommunications except where authorised in special circumstances or for the purpose of tracing the location of callers in emergencies, and for other purposes.

Chapter 1—Introduction

Part 1-1—Preliminary

1 Short title

This Act may be cited as the *Telecommunications (Interception and Access) Act 1979*.

2 Commencement

This Act shall come into operation on the day on which the *Australian Security Intelligence Organisation Act 1979* comes into operation.

4 Act binds the Crown

This Act binds the Crown in right of the Commonwealth, of each of the States, of the Australian Capital Territory and of the Northern Territory.

4A Application of the *Criminal Code*

Chapter 2 of the *Criminal Code* applies to all offences against this Act.

Note: Chapter 2 of the *Criminal Code* sets out the general principles of criminal responsibility.

Section 4B

4B Application to Norfolk Island

- (1) This Act does not extend to Norfolk Island.
- (2) Subsection (1) ceases to be in force when the *Telecommunications Act 1992* (Norfolk Island) is repealed.

Note: Once subsection (1) ceases to be in force this Act will extend to Norfolk Island because of section 18 of the *Norfolk Island Act 1979*.

Part 1-2—Interpretation

5 Interpretation

(1) In this Act, unless the contrary intention appears:

ACC means the Australian Crime Commission.

ACC Act means the *Australian Crime Commission Act 2002*.

access, in relation to a stored communication, has the meaning given by section 6AA. This definition does not apply to Schedule 1.

accessible, in relation to a communication, has the meaning given by section 5H.

access request has the meaning given by subsection 107P(1).

ACMA means the Australian Communications and Media Authority.

activities prejudicial to security has the same meaning as it has in the *Australian Security Intelligence Organisation Act 1979*.

affidavit includes affirmation.

AFP employee has the same meaning as in the *Australian Federal Police Act 1979*.

AFP Minister has the meaning given by section 100.1 of the *Criminal Code*.

agency means:

- (a) except in Chapter 2—an interception agency or another enforcement agency; or
- (b) in Chapter 2—an interception agency.

ancillary offence means an offence constituted by:

Section 5

- (a) aiding, abetting, counselling or procuring the commission of an offence;
- (b) being, by act or omission, in any way, directly or indirectly, knowingly concerned in, or party to, the commission of an offence;
- (c) receiving or assisting a person who is, to the offender's knowledge, guilty of an offence, in order to enable the person to escape punishment or to dispose of the proceeds of the last-mentioned offence;
- (d) attempting or conspiring to commit an offence; or
- (e) inciting, urging, aiding or encouraging, or printing or publishing any writing that incites, urges, aids or encourages, the commission of an offence or the carrying on of any operations for or by the commission of an offence.

appropriately used, in relation to a computer network that is operated by, or on behalf of, a Commonwealth agency, security authority or eligible authority of a State, has the meaning given by section 6AAA.

ASIC means the Australian Securities and Investments Commission.

ASIO affiliate has the same meaning as in the *Australian Security Intelligence Organisation Act 1979*.

ASIO computer access intercept information means information obtained under:

- (a) an ASIO computer access warrant; or
- (b) subsection 25A(8) of the *Australian Security Intelligence Organisation Act 1979*; or
- (c) subsection 27A(3C) of the *Australian Security Intelligence Organisation Act 1979*; or
- (d) an authorisation under section 27E of the *Australian Security Intelligence Organisation Act 1979*; or
- (e) subsection 27E(6) of the *Australian Security Intelligence Organisation Act 1979*;

by intercepting a communication passing over a telecommunications system.

ASIO computer access warrant means:

- (a) a warrant issued under section 25A of the *Australian Security Intelligence Organisation Act 1979*; or
- (b) a warrant issued under section 27A of the *Australian Security Intelligence Organisation Act 1979* that authorises the Organisation to do any of the acts or things referred to in subsection 25A(4) or (8) of that Act; or
- (c) an authorisation under section 27E of the *Australian Security Intelligence Organisation Act 1979*.

ASIO employee has the same meaning as in the *Australian Security Intelligence Organisation Act 1979*.

Assistant Integrity Commissioner has the same meaning as in the *Law Enforcement Integrity Commissioner Act 2006*.

associate, with a criminal organisation or a member of such an organisation, includes:

- (a) be in the company of the organisation or member; and
- (b) communicate with the organisation or member by any means (including by post, fax, telephone, or by email or other electronic means).

Australian Capital Territory includes the Jervis Bay Territory.

authorised officer:

- (a) in sections 180A, 180B, 180C and 180D, subsections 184(5) and 185(2) and paragraph 186(1)(ca), means:
 - (i) the Commissioner of Police; or
 - (ii) a Deputy Commissioner of Police; or
 - (iii) a member of the Australian Federal Police who is covered by an authorisation in force under subsection 5AB(1A); and
- (b) in any other case, means:

Section 5

- (i) the head (however described) of the enforcement agency or a person acting as that head; or
- (ii) a deputy head (however described) of the enforcement agency or a person acting as that deputy head; or
- (iii) a person who holds, or is acting in, an office or position in the enforcement agency that is covered by an authorisation in force under subsection 5AB(1).

authorised representative of a carrier means one of the following persons:

- (a) the Managing Director of the carrier;
- (b) the secretary of the carrier;
- (c) an employee of the carrier authorised in writing for the purposes of this paragraph by the Managing Director or the secretary of the carrier.

authority, in relation to a State, includes:

- (a) a Minister of that State;
- (b) an officer of that State;
- (c) an authority or body established for a public purpose by or under a law of that State; and
- (d) without limiting the generality of paragraph (c), the Police Force of that State.

Board of the ACC means the Board of the Australian Crime Commission established under section 7B of the ACC Act.

carriage service provider has the meaning given by the *Telecommunications Act 1997*.

carrier means:

- (a) except in Parts 5-4 and 5-4A:
 - (i) a carrier (within the meaning of the *Telecommunications Act 1997*); or
 - (ii) a carriage service provider; and
- (b) in Parts 5-4 and 5-4A—a carrier (within the meaning of the *Telecommunications Act 1997*).

carry includes transmit, switch and receive.

certifying officer, in relation to an agency, or an eligible authority of a State, means:

- (a) in the case of the Australian Federal Police—the Commissioner of Police, a Deputy Commissioner of Police or a person authorised to be a certifying officer of the Australian Federal Police under subsection 5AC(1); or
- (aa) in the case of the Australian Commission for Law Enforcement Integrity:
 - (i) the Integrity Commissioner; or
 - (ii) an Assistant Integrity Commissioner; or
 - (iii) a person authorised to be a certifying officer of ACLEI under subsection 5AC(2); or
- (b) in the case of the ACC:
 - (i) the Chief Executive Officer of the ACC or an examiner; or
 - (ii) a person authorised to be a certifying officer of the ACC under subsection 5AC(3); or
- (c) in the case of the Police Force of a State—the Commissioner, a Deputy Commissioner, an officer whose rank is equivalent to that of Assistant Commissioner of the Australian Federal Police, or a person authorised to be a certifying officer of the Police Force of the State under subsection 5AC(4); or
- (d) in the case of the Crime Commission:
 - (i) a member of the Crime Commission; or
 - (ii) a person authorised to be a certifying officer of the Crime Commission under subsection 5AC(5); or
- (e) in the case of the Independent Commission Against Corruption:
 - (i) the Chief Commissioner, a Commissioner or an Assistant Commissioner of the Independent Commission Against Corruption; or
 - (ii) a person authorised to be a certifying officer of the Independent Commission Against Corruption under subsection 5AC(6); or

Section 5

- (ea) in the case of the IBAC:
 - (i) the Commissioner of the IBAC; or
 - (ii) the Deputy Commissioner of the IBAC; or
 - (iii) a person authorised to be a certifying officer of the IBAC under subsection 5AC(7); or
- (f) in the case of the Crime and Corruption Commission:
 - (i) the chairman (as defined by the Crime and Corruption Act); or
 - (ii) a senior executive officer (as defined by the Crime and Corruption Act); or
- (g) in the case of the Law Enforcement Conduct Commission:
 - (i) the Chief Commissioner of the Commission; or
 - (ii) the Commissioner for Integrity of the Commission; or
 - (iii) a person authorised to be a certifying officer of the Commission under subsection 5AC(8); or
- (i) in the case of the Corruption and Crime Commission:
 - (i) the Commissioner of the Corruption and Crime Commission; or
 - (ii) a person authorised to be a certifying officer of the Corruption and Crime Commission under subsection 5AC(9); or
- (ia) in the case of the Independent Commissioner Against Corruption:
 - (i) the Independent Commissioner Against Corruption; or
 - (ii) the Deputy Commissioner referred to in section 9 of the Independent Commissioner Against Corruption Act; or
 - (iii) a person authorised to be a certifying officer for the Independent Commissioner Against Corruption under subsection 5AC(9A); or
- (j) in the case of any other agency:
 - (i) the chief executive officer or an acting chief executive officer of the agency; or
 - (ii) a person authorised to be a certifying officer of the agency under subsection 5AC(10).

certifying official, of an issuing agency, means:

- (a) if the issuing agency is an enforcement agency (including an interception agency)—a certifying officer of the agency; and
- (b) if the issuing agency is the Organisation—a certifying person of the Organisation.

certifying person means any of the following:

- (a) the Director-General of Security;
- (b) a Deputy Director-General of Security;
- (c) a person authorised to be a certifying person of the Organisation under section 5AD.

chief officer, in relation to an agency, an eligible Commonwealth authority or an eligible authority of a State, means:

- (a) in the case of the Australian Federal Police—the Commissioner of Police; or
- (aa) in the case of the Australian Commission for Law Enforcement Integrity—the Integrity Commissioner; or
- (b) in the case of the ACC—the Chief Executive Officer of the ACC; or
- (ba) in the case of an eligible Commonwealth authority—the member constituting, or the member who generally presides at hearings and other meetings of, the Commonwealth Royal Commission concerned; or
- (c) in the case of the Police Force of a State—the Commissioner of that Police Force; or
- (d) in the case of the Crime Commission—the Commissioner of the Crime Commission; or
- (e) in the case of the Independent Commission Against Corruption—the Chief Commissioner of the Independent Commission Against Corruption; or
- (ea) in the case of the Inspector of the Independent Commission Against Corruption—the Inspector of the Independent Commission Against Corruption; or
- (eb) in the case of the IBAC—the Commissioner of the IBAC; or

Section 5

- (ec) in the case of the Victorian Inspectorate—the Inspector of the Victorian Inspectorate; or
- (f) in the case of the Crime and Corruption Commission—the chairman of the Commission; or
- (h) in the case of the Law Enforcement Conduct Commission—the Chief Commissioner of the Commission; or
- (ha) in the case of the Inspector of the Law Enforcement Conduct Commission—the Inspector; or
- (k) in the case of the Corruption and Crime Commission—the Commissioner of the Commission; or
- (l) in the case of the Parliamentary Inspector of the Corruption and Crime Commission—the Parliamentary Inspector of the Corruption and Crime Commission; or
- (la) in the case of the Independent Commissioner Against Corruption—the Independent Commissioner Against Corruption; or
- (m) in the case of an enforcement agency that is not an interception agency and is not an eligible authority of a State—the chief executive officer or an acting chief executive officer of the agency.

Commissioner means:

- (a) in relation to the Police Force of a State—the Commissioner of Police (however designated) of that State; or
- (b) in relation to the Crime and Corruption Commission—a member of the Commission, including the chairman.

Commissioner of Police means the Commissioner of Police referred to in section 6 of the *Australian Federal Police Act 1979*, and includes an acting Commissioner of Police.

Commonwealth agency means:

- (a) the Australian Federal Police; or
- (aa) the Australian Commission for Law Enforcement Integrity;
or
- (b) the ACC.

Commonwealth Royal Commission means a Royal Commission within the meaning of the *Royal Commissions Act 1902*.

communicate, in relation to information, includes divulge.

communication includes conversation and a message, and any part of a conversation or message, whether:

- (a) in the form of:
 - (i) speech, music or other sounds;
 - (ii) data;
 - (iii) text;
 - (iv) visual images, whether or not animated; or
 - (v) signals; or
- (b) in any other form or in any combination of forms.

Communications Access Co-ordinator has the meaning given by section 6R.

conduct includes any act or omission.

confirmed control order has the same meaning as in Part 5.3 of the *Criminal Code*.

connected with: a purpose is **connected with** a preventative detention order law if the purpose is connected with the performance of a function or duty, or the exercise of a power, by a person, court, tribunal or other body under, or in relation to a matter arising under, that law, so far as the function, duty or power relates to a preventative detention order (within the meaning of that law).

control order has the same meaning as in Part 5.3 of the *Criminal Code*.

Corruption and Crime Commission means the Corruption and Crime Commission established by the Corruption and Crime Commission Act.

Section 5

Corruption and Crime Commission Act means the *Corruption and Crime Commission Act 2003* of Western Australia.

Crime and Corruption Act means the *Crime and Corruption Act 2001* (Qld).

Crime and Corruption Commission means the Crime and Corruption Commission (Qld).

Crime Commission means the New South Wales Crime Commission.

Crime Commission Act means the *New South Wales Crime Commission Act 1985* of New South Wales.

crime within the jurisdiction of the ICC has the same meaning as in the *International Criminal Court Act 2002*.

criminal law-enforcement agency has the meaning given by section 110A.

criminal organisation means an organisation (whether incorporated or not, and however structured) that is:

- (a) a declared organisation within the meaning of:
 - (i) the *Crimes (Criminal Organisations Control) Act 2009* of New South Wales; or
 - (ii) the *Serious and Organised Crime (Control) Act 2008* of South Australia; or
- (b) an organisation of a kind specified by or under, or described or mentioned in, a prescribed provision of a law of a State or Territory.

data disruption intercept information means information obtained under a data disruption warrant by intercepting a communication passing over a telecommunications system.

data disruption warrant has the same meaning as in the *Surveillance Devices Act 2004*.

Defence Minister has the same meaning as in the *Intelligence Services Act 2001*.

delivery point means a location in respect of which a nomination or determination is in force under section 188.

Deputy Commissioner of Police means a Deputy Commissioner of Police referred to in section 6 of the *Australian Federal Police Act 1979*.

Deputy Director-General of Security means a person who holds, or is acting in, a position known as Deputy Director-General of Security.

deputy PIM (short for deputy public interest monitor), in relation to Queensland, means a person appointed as a deputy public interest monitor under:

- (a) the *Crime and Corruption Act 2001* of Queensland; or
- (b) the *Police Powers and Responsibilities Act 2000* of Queensland.

detained in custody in a prison has the meaning given by section 100.1 of the *Criminal Code*.

Director-General of Security means the person holding, or performing the duties of, the office of Director-General of Security under the *Australian Security Intelligence Organisation Act 1979*.

domestic preservation notice has the meaning given by subsection 107H(1).

earth-based facility means a facility other than a satellite-based facility.

eligible authority, in relation to a State, means:

- (a) in any case—the Police Force of that State; or
- (b) in the case of New South Wales:
 - (i) the Crime Commission; or
 - (ii) the Independent Commission Against Corruption; or

Section 5

- (iii) the Inspector of the Independent Commission Against Corruption; or
- (iv) the Law Enforcement Conduct Commission; or
- (v) the Inspector of the Law Enforcement Conduct Commission; or
- (ba) in the case of Victoria—the IBAC or the Victorian Inspectorate; or
- (c) in the case of Queensland—the Crime and Corruption Commission; or
- (d) in the case of Western Australia—the Corruption and Crime Commission or the Parliamentary Inspector of the Corruption and Crime Commission; or
- (e) in the case of South Australia—the Independent Commissioner Against Corruption.

eligible Commonwealth authority means a Commonwealth Royal Commission in relation to which a declaration under section 5AA is in force.

emergency service facility has the meaning given by subsection 6(2A).

enforcement agency has the meaning given by section 176A.

engage in a hostile activity has the same meaning as in Part 5.3 of the *Criminal Code*.

equipment means any apparatus or equipment used, or intended for use, in or in connection with a telecommunications network, and includes a telecommunications device but does not include a line. This definition does not apply to Schedule 1.

examiner has the same meaning as in the ACC Act.

extended supervision order has the meaning given by section 105A.2 of the *Criminal Code*.

facility has the same meaning as in the *Telecommunications Act 1997*.

federally relevant criminal activity has the same meaning as in the ACC Act.

Foreign Affairs Minister has the same meaning as in the *Intelligence Services Act 2001*.

foreign communication means a communication sent or received outside Australia.

foreign communications warrant means an interception warrant issued or to be issued under section 11C.

foreign country, when used in the expression ***hostile activity in a foreign country***, has the same meaning as in the *Criminal Code*.

foreign intelligence means intelligence about the capabilities, intentions or activities of people or organisations outside Australia.

foreign intelligence information means information obtained (whether before or after the commencement of this definition) under a warrant issued under section 11A, 11B or 11C.

foreign law enforcement agency means:

- (a) a police force (however described) of a foreign country; or
- (b) any other authority or person responsible for the enforcement of the laws of the foreign country; or
- (c) any other authority or person responsible to the International Criminal Court for investigating or prosecuting a crime within the jurisdiction of the ICC; or
- (d) any other authority or person responsible to a War Crimes Tribunal for investigating or prosecuting a War Crimes Tribunal offence.

foreign organisation means an organisation (including a government) outside Australia.

foreign power has the same meaning as in the *Australian Security Intelligence Organisation Act 1979*.

Section 5

foreign preservation notice has the meaning given by subsection 107N(1).

general computer access intercept information means information obtained under a general computer access warrant by intercepting a communication passing over a telecommunications system.

general computer access warrant means a warrant issued under section 27C of the *Surveillance Devices Act 2004*.

General Register means the General Register of Warrants kept under section 81A.

Governor, in relation to a State, means, in the case of the Northern Territory, the Administrator of the Northern Territory.

historic domestic preservation notice has the meaning given by subparagraph 107H(1)(b)(i).

IBAC means the Independent Broad-based Anti-corruption Commission established by the IBAC Act.

IBAC Act means the *Independent Broad-based Anti-corruption Commission Act 2011* of Victoria.

IBAC officer means a person who is an IBAC Officer (within the meaning of the IBAC Act).

IGIS official has the same meaning as in the *Australian Security Intelligence Organisation Act 1979*.

Immigration and Border Protection Department means the Department administered by the Minister administering Part XII of the *Customs Act 1901*.

immigration offence means an offence against section 236 of the *Migration Act 1958*.

implementation phase has the meaning given by subsection 187H(2).

Independent Commission Against Corruption means the Independent Commission Against Corruption of New South Wales.

Independent Commission Against Corruption Act means the *Independent Commission Against Corruption Act 1988* of New South Wales.

Independent Commissioner Against Corruption means the person who is the Commissioner (within the meaning of the Independent Commissioner Against Corruption Act).

Independent Commissioner Against Corruption Act means the *Independent Commissioner Against Corruption Act 2012* of South Australia.

infrastructure means any line or equipment used to facilitate communications across a telecommunications network.

inspecting officer means:

- (a) the Ombudsman;
- (b) a Deputy Commonwealth Ombudsman; or
- (c) a member of the staff referred to in subsection 31(1) of the *Ombudsman Act 1976*.

Inspector of the Independent Commission Against Corruption means the Inspector of the Independent Commission Against Corruption referred to in section 57A of the Independent Commission Against Corruption Act.

Inspector of the Law Enforcement Conduct Commission has the same meaning as ***Inspector*** has in the *Law Enforcement Conduct Commission Act 2016* (NSW).

Inspector of the Victorian Inspectorate has the same meaning as ***Inspector*** has in the Victorian Inspectorate Act.

integrity authority means:

- (a) an integrity testing controlled operations authority under Part IAB of the *Crimes Act 1914* authorising a controlled operation under that Part; or

Section 5

- (b) an integrity testing authority under Part IABA of the *Crimes Act 1914* authorising an integrity testing operation under that Part.

Integrity Commissioner has the same meaning as in the *Law Enforcement Integrity Commissioner Act 2006*.

integrity operation means:

- (a) a controlled operation authorised by an integrity testing controlled operation authority granted under Part IAB of the *Crimes Act 1914*; or
- (b) an integrity testing operation authorised by an integrity testing authority granted under Part IABA of the *Crimes Act 1914*.

intended recipient, of a communication, (except when used in Schedule 1) has the meaning given by section 5G.

interception agency means:

- (a) except for the purposes of section 6R, Part 2-6 or Chapter 5:
- (i) a Commonwealth agency; or
 - (ii) an eligible authority of a State in relation to which a declaration under section 34 is in force; or
- (b) for the purposes of Part 2-6:
- (i) a Commonwealth agency; or
 - (ii) an eligible authority of a State; or
- (c) for the purposes of section 6R and Chapter 5:
- (i) the Organisation; or
 - (ii) a Commonwealth agency; or
 - (iii) an eligible authority of a State in relation to which a declaration under section 34 is in force.

interception warrant means a warrant issued under Chapter 2.

interception warrant information has the meaning given by section 6EA.

interim control order has the same meaning as in Part 5.3 of the *Criminal Code*.

interim supervision order has the meaning given by section 105A.2 of the *Criminal Code*.

international assistance application means an application for a stored communications warrant made as a result of:

- (a) an authorisation under section 15B of the *Mutual Assistance in Criminal Matters Act 1987*; or
- (b) an authorisation under section 78A of the *International Criminal Court Act 2002*; or
- (c) an authorisation under section 34A of the *International War Crimes Tribunals Act 1995*.

International Criminal Court has the same meaning as **ICC** in the *International Criminal Court Act 2002*.

international offence has the meaning given by subsection 162(3).

in the possession of, in relation to a document, record or copy, includes in the custody of or under the control of.

investigative proceeding has the same meaning as in the *Mutual Assistance in Criminal Matters Act 1987*.

issuing agency, in relation to a preservation notice, means the agency that gives the notice.

issuing authority (except when used in Schedule 1) means a person in respect of whom an appointment is in force under section 6DB.

journalist information warrant means a warrant issued under Division 4C of Part 4-1.

Law Enforcement Conduct Commission means the Law Enforcement Conduct Commission constituted by the *Law Enforcement Conduct Commission Act 2016* (NSW).

Section 5

lawfully accessed information means information obtained by accessing a stored communication otherwise than in contravention of subsection 108(1), but does not include information obtained in accordance with an international production order (within the meaning of Schedule 1).

lawfully intercepted information has the meaning given by section 6E.

law of the Commonwealth includes a law of the Australian Capital Territory.

line has the same meaning as in the *Telecommunications Act 1997*.

listening device has the same meaning as in Division 2 of Part III of the *Australian Security Intelligence Organisation Act 1979*.

maintain includes adjust and repair.

main unexplained wealth provisions has the same meaning as in the *Proceeds of Crime Act 2002*.

Managing Director, in relation to a carrier, means the chief executive officer (however described) of the carrier.

member, of a criminal organisation, includes:

- (a) in the case of an organisation that is a body corporate—a director and an officer of the body corporate; and
- (b) in any case:
 - (i) an associate member or prospective member (however described) of the organisation; and
 - (ii) a person who identifies himself or herself, in some way, as belonging to the organisation; and
 - (iii) a person who is treated by the organisation or persons who belong to the organisation, in some way, as if he or she belongs to the organisation.

member of a police force means:

- (a) a member of the Australian Federal Police; or
- (b) an officer of the Police Force of a State or Territory.

member of the Australian Federal Police includes a special member of the Australian Federal Police.

member of the Crime Commission means a person who is, or who is acting in the office of, the Chairperson, or a member, of the Crime Commission.

member of the staff of a Commonwealth Royal Commission means:

- (a) a legal practitioner appointed to assist the Commission; or
- (b) a person authorised to be a member of the staff of a Commonwealth Royal Commission for the purposes of this Act under section 5AE.

member of the staff of the ACC has the same meaning as in the ACC Act.

member of the staff of the Crime Commission means a person who is, for the purposes of the Crime Commission Act, a member of the staff of the Crime Commission.

member of the staff of the Independent Commissioner Against Corruption means a person who is engaged under subsection 12(1) of the Independent Commissioner Against Corruption Act.

member of the staff of the Inspector of the Independent Commission Against Corruption means:

- (a) a member of the staff referred to in subsection 57E(1) or (2) of the Independent Commission Against Corruption Act; or
- (b) a person engaged under subsection 57E(3) of that Act; or
- (c) a person whose services are used under subsection 57E(4) of that Act.

member of the staff of the Inspector of the Law Enforcement Conduct Commission means a member of staff of the Inspector

Section 5

(within the meaning of the *Law Enforcement Conduct Commission Act 2016* (NSW)).

member of the staff of the Law Enforcement Conduct Commission means a member of staff of the Commission (within the meaning of the *Law Enforcement Conduct Commission Act 2016* (NSW)).

Minister, in relation to a State, means:

- (a) except where paragraph (b) applies—a Minister of the Crown of that State; or
- (b) in the case of the Northern Territory—a person holding Ministerial office within the meaning of the *Northern Territory (Self-Government) Act 1978*.

Minister for Defence means the Minister administering the *Defence Act 1903*.

Minister for Foreign Affairs means the Minister administering the *Diplomatic Privileges and Immunities Act 1967*.

missing person information, in relation to a missing person, has the meaning given by section 182.

named person warrant means an interception warrant issued or to be issued under section 9A, 11B or 46A.

network activity warrant has the same meaning as in the *Surveillance Devices Act 2004*.

network activity warrant intercept information means information obtained under a network activity warrant by intercepting a communication passing over a telecommunications system.

network protection duties, in relation to a computer network, means duties relating to:

- (a) the operation, protection or maintenance of the network; or
- (b) if the network is operated by, or on behalf of, a Commonwealth agency, security authority or eligible authority of a State—ensuring that the network is

appropriately used by employees, office holders or contractors of the agency or authority.

nominated AAT member (except when used in Schedule 1) means a member of the Administrative Appeals Tribunal in respect of whom a nomination is in force under section 6DA to issue warrants under Part 2-5.

nominated carriage service provider means a carriage service provider covered by a declaration in force under subsection 197(4).

non-missing person information has the meaning given by section 182.

notifiable equipment, in relation to a carrier or nominated carriage service provider, means equipment that:

- (a) provides all or part of the carrier or provider's telecommunication services; or
- (b) manages all or part of the provision of the carrier or provider's telecommunication services; or
- (c) manages some or all of the information to which section 276 of the *Telecommunications Act 1997* applies in relation to the carrier or provider.

oath includes affirmation.

offence means an offence against a law of the Commonwealth or of a State.

office holder means a person who holds, occupies or performs the duties of an office, position or appointment.

officer, in relation to an agency, an eligible Commonwealth authority or an eligible authority of a State, means:

- (a) in the case of the Australian Federal Police—a member of the Australian Federal Police; or
- (aa) in the case of the Australian Commission for Law Enforcement Integrity—the Integrity Commissioner or a staff member of ACLEI; or

Section 5

- (b) in the case of the ACC—the Chief Executive Officer of the ACC, an examiner or a member of the staff of the ACC; or
- (ba) in the case of an eligible Commonwealth authority—a member of the Commonwealth Royal Commission concerned or a member of the staff of the Royal Commission; or
- (c) in the case of the Police Force of a State—an officer of that Police Force; or
- (d) in the case of the Crime Commission—a member of the Crime Commission or a member of the staff of the Crime Commission; or
- (e) in the case of the Independent Commission Against Corruption—an officer of the Independent Commission Against Corruption, being a person who is an officer as defined by the Independent Commission Against Corruption Act; or
- (ea) in the case of the Inspector of the Independent Commission Against Corruption:
 - (i) the Inspector of the Independent Commission Against Corruption; or
 - (ii) a member of the staff of the Inspector of the Independent Commission Against Corruption; or
- (eb) in the case of the IBAC—an IBAC officer; or
- (ec) in the case of the Victorian Inspectorate—a Victorian Inspectorate officer; or
- (f) in the case of the Crime and Corruption Commission—a commission officer (within the meaning of the Crime and Corruption Act); or
- (h) in the case of the Law Enforcement Conduct Commission:
 - (i) the Chief Commissioner of the Commission; or
 - (ii) the Commissioner for Integrity of the Commission; or
 - (iii) an Assistant Commissioner of the Commission; or
 - (iv) a member of the staff of the Law Enforcement Conduct Commission; or

- (ha) in the case of the Inspector of the Law Enforcement Conduct Commission:
 - (i) the Inspector; or
 - (ii) an Assistant Inspector of the Commission; or
 - (iii) a member of the staff of the Inspector of the Law Enforcement Conduct Commission; or
- (k) in the case of the Corruption and Crime Commission—an officer of the Corruption and Crime Commission; or
- (l) in the case of the Parliamentary Inspector of the Corruption and Crime Commission—the Parliamentary Inspector of the Corruption and Crime Commission or an officer of the Parliamentary Inspector; or
- (m) in the case of the Independent Commissioner Against Corruption:
 - (i) the Independent Commissioner Against Corruption; or
 - (ii) the Deputy Commissioner referred to in section 9 of the Independent Commissioner Against Corruption Act; or
 - (iii) a member of the staff of the Independent Commissioner Against Corruption; or
- (n) in the case of a criminal law-enforcement agency for which a declaration under subsection 110A(3) is in force—a person specified, or of a kind specified, in the declaration to be an officer of the criminal law-enforcement agency for the purposes of this Act; or
- (o) in the case of an enforcement agency for which a declaration under subsection 176A(3) is in force—a person specified, or of a kind specified, in the declaration to be an officer of the enforcement agency for the purposes of this Act.

officer of a State has the meaning given by subsection 6G(2).

officer of a Territory has the meaning given by subsection 6G(3).

officer of the Commonwealth has the meaning given by subsection 6G(1).

Section 5

officer of the Corruption and Crime Commission means an officer of the Corruption and Crime Commission within the meaning of the Corruption and Crime Commission Act.

officer of the Parliamentary Inspector means an officer of the Parliamentary Inspector of the Corruption and Crime Commission within the meaning of the Corruption and Crime Commission Act.

Ombudsman means the Commonwealth Ombudsman.

Ombudsman official means:

- (a) the Ombudsman; or
- (b) a Deputy Commonwealth Ombudsman; or
- (c) a person who is a member of the staff referred to in subsection 31(1) of the *Ombudsman Act 1976*.

ongoing domestic preservation notice has the meaning given by subparagraph 107H(1)(b)(ii).

Organisation means the Australian Security Intelligence Organisation.

organised crime control law means a law of a State, a purpose of which is to combat organised crime or restrict the activities of criminal organisations, that provides for:

- (a) the declaration of an organisation as a declared organisation; or
- (b) the making of orders described as control orders or interim control orders in relation to members of criminal organisations.

original warrant means a warrant other than a renewal of a warrant.

Parliamentary Inspector of the Corruption and Crime Commission means the Parliamentary Inspector of the Corruption and Crime Commission within the meaning of the Corruption and Crime Commission Act.

Part 2-2 warrant means a warrant issued under Part 2-2.

Part 2-5 warrant means a warrant issued under Part 2-5.

Part 4-1 issuing authority means a person in respect of whom an appointment is in force under section 6DC.

Part 5.3 object means:

- (a) in relation to a control order—any of the following:
 - (i) the protection of the public from a terrorist act;
 - (ii) the prevention of the provision of support for, or the facilitation of, a terrorist act;
 - (iii) the prevention of the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country; or
- (b) in relation to an extended supervision order or interim supervision order—the protection of the community from the unacceptable risk of a terrorist offender committing a serious Part 5.3 offence.

Part 5.3 supervisory order means:

- (a) a control order; or
- (b) an extended supervision order or interim supervision order.

Part 5.3 warrant means a warrant issued:

- (a) under subsection 46(4) or (7) or 46A(2A) or (2C); or
- (b) under section 48 in the circumstances mentioned in subsection 46(4) or (7).

Part 5.3 warrant agency means:

- (a) a Commonwealth agency; or
- (b) an eligible authority of a State that a declaration in force under section 34 authorises to apply for Part 5.3 warrants (see section 38A).

participating State has the same meaning as in the *Proceeds of Crime Act 2002*.

passing over includes being carried.

Section 5

Note: See section 5F for when a communication is passing over a telecommunications system.

permitted purpose, in relation to an interception agency, the Immigration and Border Protection Department, an eligible Commonwealth authority, an eligible authority of a State or ASIC, means a purpose connected with:

- (a) in any case (except in the case of the Immigration and Border Protection Department or ASIC):
 - (i) an investigation by the agency or eligible authority of a prescribed offence;
 - (ii) the making by an authority, body or person of a decision whether or not to begin a relevant proceeding in relation to the agency or eligible authority;
 - (iii) a relevant proceeding in relation to the agency or eligible authority;
 - (iv) the exercise by the chief officer of the agency or eligible authority of the powers conferred by section 68; or
 - (v) the keeping of records by the agency under Part 2-7, or by the eligible authority under provisions of a law of the State that impose on the chief officer of the authority requirements corresponding to those imposed on the chief officer of a Commonwealth agency by sections 80 and 81; or
- (aaa) in the case of a Commonwealth agency or the Immigration and Border Protection Department—a purpose mentioned in the table in section 6S in relation to the agency or the Immigration and Border Protection Department; or
- (aa) in the case of the ACC:
 - (i) a special ACC operation/investigation; or
 - (ii) a report to the Board of the ACC on the outcome of such an operation or investigation; or
 - (iii) an investigation of, or an inquiry into, alleged misbehaviour, or alleged improper conduct, of a member of the staff referred to in subsection 47(1) of the *Australian Crime Commission Act 2002*; or
 - (iv) a report on such an investigation or inquiry; or

- (v) the making by a person of a decision, following such an investigation or inquiry, in relation to the employment of such a staff member (including a decision to terminate the staff member's employment); or
 - (vi) a review (whether by way of appeal or otherwise) of such a decision; or
- (b) in the case of the Australian Federal Police:
- (i) an investigation of, or an inquiry into, alleged misbehaviour, or alleged improper conduct, of an officer of the Commonwealth, being an investigation or inquiry under a law of the Commonwealth or by a person in the person's capacity as an officer of the Commonwealth; or
 - (ii) a report on such an investigation or inquiry; or
 - (iia) the making by a person of a decision under the *Australian Federal Police Act 1979* in relation to the engagement of an AFP employee, the retirement of an AFP employee or the termination of the employment of an AFP employee or in relation to the appointment or the termination of the appointment of a special member of the Australian Federal Police; or
 - (iib) a review (whether by way of appeal or otherwise) of such a decision; or
 - (iic) the tendering to the Governor-General of advice to terminate, because of misbehaviour or improper conduct, the appointment of an officer of the Commonwealth; or
 - (iv) deliberations of the Executive Council in connection with advice to the Governor-General to terminate, because of misbehaviour or improper conduct, the appointment of an officer of the Commonwealth; or
 - (v) the performance of a function or duty, or the exercise of a power, by a person, court or other body under, or in relation to a matter arising under, Division 104 (control orders) or Division 105A (post-sentence orders) of the *Criminal Code*; or

Section 5

- (vi) a preventative detention order law; or
- (vii) a post-sentence detention law or a post-sentence supervision law; or
- (viii) the making of a decision whether to apply for a post-sentence order, or for a variation or review of a post-sentence order, under Division 105A of the *Criminal Code* in relation to a person; or
- (ix) the making of a decision whether to apply for an order, or make any other application in relation to an order, under a post-sentence detention law or a post-sentence supervision law in relation to a person; or
- (baa) in the case of the Australian Commission for Law Enforcement Integrity:
 - (i) a corruption investigation (within the meaning of the *Law Enforcement Integrity Commissioner Act 2006*); or
 - (ii) a report on such an investigation; or
- (bab) in the case of an eligible Commonwealth authority:
 - (i) an investigation that the Commonwealth Royal Commission concerned is conducting in the course of the inquiry it is commissioned to undertake; or
 - (ii) a report on such an investigation; or
- (c) in the case of the Police Force of a State:
 - (i) an investigation of, or an inquiry into, alleged misbehaviour, or alleged improper conduct, of an officer of that State, being an investigation or inquiry under a law of that State or by a person in the person's capacity as an officer of that State; or
 - (ii) a report on such an investigation or inquiry; or
- (ia) the making by a person of a decision in relation to the appointment, re-appointment, term of appointment, retirement or termination of appointment of an officer or member of staff of that Police Force; or
- (iab) a review (whether by way of appeal or otherwise) of such a decision; or

- (iii) the tendering to the Governor of that State of advice to terminate, because of misbehaviour or improper conduct, the appointment of an officer of that State; or
 - (iv) deliberations of the Executive Council of that State in connection with advice to the Governor of that State to terminate, because of misbehaviour or improper conduct, the appointment of an officer of that State; or
 - (v) the performance of a function or duty, or the exercise of a power, by a person, court or other body under, or in relation to a matter arising under, an organised crime control law of that State; or
 - (vi) the performance of a function or duty, or the exercise of a power, by a person, court or other body under, or in relation to a matter arising under, Division 104 (control orders) or Division 105A (post-sentence orders) of the *Criminal Code*; or
 - (vii) a preventative detention order law; or
 - (viii) a post-sentence detention law or a post-sentence supervision law; or
 - (ix) the making of a decision whether to apply for a post-sentence order, or for a variation or review of a post-sentence order, under Division 105A of the *Criminal Code* in relation to a person; or
 - (x) the making of a decision whether to apply for an order, or make any other application in relation to an order, under a post-sentence detention law or a post-sentence supervision law in relation to a person; or
- (d) in the case of an eligible authority of a State:
- (i) an inspection of the authority's records that is made under a requirement of the law of that State, being a requirement of the kind referred to in paragraph 35(1)(h); or
 - (ii) a report on such an inspection; or
- (da) in the case of the Independent Commission Against Corruption:

Section 5

- (i) an investigation under the Independent Commission Against Corruption Act into whether corrupt conduct (within the meaning of that Act) may have occurred, may be occurring or may be about to occur; or
- (ii) a report on such an investigation; or
- (db) in the case of the Inspector of the Independent Commission Against Corruption:
 - (i) dealing with (by reports and recommendations) complaints of abuse of power, impropriety or other forms of misconduct (within the meaning of the Independent Commission Against Corruption Act) on the part of the Independent Commission Against Corruption or officers of that Commission; or
 - (ii) dealing with (by reports and recommendations) conduct amounting to maladministration (within the meaning of the Independent Commission Against Corruption Act) by the Independent Commission Against Corruption or officers of that Commission; or
- (dc) in the case of the Inspector of the Law Enforcement Conduct Commission—dealing with (by reports and recommendations) conduct amounting to:
 - (i) agency maladministration (within the meaning of subsection (6A)) on the part of the Commission; or
 - (ii) officer misconduct (within the meaning of section 122 of the *Law Enforcement Conduct Commission Act 2016* (NSW)) or officer maladministration (within the meaning of that section) on the part of officers (within the meaning of that Act) of the Commission;
whether or not the subject of a complaint; or
- (e) in the case of the Law Enforcement Conduct Commission:
 - (i) an investigation under Part 6 of the *Law Enforcement Conduct Commission Act 2016* (NSW) in respect of conduct to which subsection (7) of this section applies; or
 - (ii) a report on an investigation covered by subparagraph (i); or

- (iii) the tendering to the Governor of New South Wales of advice to terminate, because of misbehaviour or improper conduct, the appointment of the Commissioner of the New South Wales Police Force; or
- (iv) deliberations of the Executive Council of New South Wales in connection with advice to the Governor of that State to terminate, because of misbehaviour or improper conduct, the appointment of the Commissioner of the New South Wales Police Force; or
- (f) in the case of the IBAC:
 - (i) an investigation under the IBAC Act of corrupt conduct (within the meaning of that Act); or
 - (ii) an investigation under the IBAC Act of police personnel conduct (within the meaning of that Act); or
 - (iii) a report or recommendation on an investigation covered by subparagraph (i) or (ii); or
- (fa) in the case of the Victorian Inspectorate:
 - (i) an investigation under the Victorian Inspectorate Act into the conduct of the IBAC or IBAC personnel (within the meaning of that Act); or
 - (ii) a report or recommendation on such an investigation; or
- (g) in the case of the Corruption and Crime Commission:
 - (i) an investigation under the Corruption and Crime Commission Act into whether misconduct (within the meaning of that Act) has or may have occurred, is or may be occurring, is or may be about to occur, or is likely to occur; or
 - (ii) a report on such an investigation; or
- (ga) in the case of the Crime and Corruption Commission:
 - (i) an investigation under the Crime and Corruption Act into whether corruption (within the meaning of that Act) may have occurred, may be occurring or may be about to occur; or
 - (ii) a report on such an investigation; or
- (h) in the case of the Parliamentary Inspector of the Corruption and Crime Commission—dealing with a matter of

Section 5

misconduct (within the meaning of the Corruption and Crime Commission Act) on the part of the Corruption and Crime Commission, an officer of the Corruption and Crime Commission or an officer of the Parliamentary Inspector of the Corruption and Crime Commission; or

- (i) in the case of the Independent Commissioner Against Corruption:
 - (i) an investigation under the Independent Commissioner Against Corruption Act into corruption in public administration (within the meaning of that Act); or
 - (ii) a report on such an investigation; or
- (j) in the case of ASIC:
 - (i) an investigation by ASIC of a serious offence or of the likely commission of a serious offence; or
 - (ii) a report on such an investigation; or
 - (iii) the making of a decision whether or not to begin a prosecution for a serious offence if the prosecution arises from or relates to such an investigation; or
 - (iv) a prosecution for a serious offence if the prosecution arises from or relates to such an investigation.

PIM (short for public interest monitor) means:

- (a) in relation to Victoria—a person appointed as a Public Interest Monitor under the *Public Interest Monitor Act 2011* of Victoria; or
- (b) in relation to Queensland—a person appointed as the public interest monitor under:
 - (i) the *Crime and Corruption Act 2001* of Queensland; or
 - (ii) the *Police Powers and Responsibilities Act 2000* of Queensland.

police disciplinary proceeding means a disciplinary proceeding, before a tribunal or body that is responsible for disciplining members of the Australian Federal Police or officers of a Police Force of a State, against a member of the Australian Federal Police, or an officer of that Police Force, as the case may be, not being a proceeding by way of a prosecution for an offence.

post-sentence detention law means any of the following laws:

- (a) Part 3 of the *Terrorism (High Risk Offenders) Act 2017* (NSW);
- (b) Parts 5 and 6 of the *Serious Offenders Act 2018* (Vic.);
- (c) Part 3 of the *Criminal Law (High Risk Offenders) Act 2015* (SA);
- (d) any other law, or part of a law, of a State or Territory prescribed by the regulations.

post-sentence order means:

- (a) a continuing detention order or interim detention order made under Division 105A of the *Criminal Code*; or
- (b) an extended supervision order or interim supervision order.

post-sentence supervision law means any of the following laws:

- (a) Part 2 of the *Terrorism (High Risk Offenders) Act 2017* (NSW);
- (b) Parts 3 and 4 of the *Serious Offenders Act 2018* (Vic.);
- (c) Part 2 of the *Criminal Law (High Risk Offenders) Act 2015* (SA);
- (d) any other law, or part of a law, of a State or Territory prescribed by the regulations.

Premier, in relation to a State, means, in the case of the Northern Territory, the Chief Minister of the Northern Territory.

premises includes:

- (a) any land;
- (b) any structure, building, aircraft, vehicle, vessel or place (whether built on or not); and
- (c) any part of such a structure, building, aircraft, vehicle, vessel or place.

Section 5

prescribed investigation, in relation to a Commonwealth agency, an eligible Commonwealth authority or an eligible authority of a State:

- (aa) in the case of the Australian Commission for Law Enforcement Integrity—means a corruption investigation (within the meaning of the *Law Enforcement Integrity Commissioner Act 2006*); or
- (a) in the case of the ACC—means a special ACC operation/investigation; or
- (b) in the case of the Crime Commission—means an investigation that the Crime Commission is conducting in the performance of its functions under the Crime Commission Act; or
- (ba) in the case of an eligible Commonwealth authority—an investigation that the Commonwealth Royal Commission concerned is conducting in the course of the inquiry it is commissioned to undertake; or
- (c) in the case of the Independent Commission Against Corruption—means an investigation that the Independent Commission Against Corruption is conducting in the performance of its functions under the Independent Commission Against Corruption Act; or
- (ca) in the case of the Inspector of the Independent Commission Against Corruption—means an investigation that the Inspector is conducting in the performance of the Inspector’s functions under the Independent Commission Against Corruption Act; or
- (cb) in the case of the IBAC—means an investigation that the IBAC is conducting in the performance of its functions under the IBAC Act; or
- (cc) in the case of the Victorian Inspectorate—means an investigation that the Victorian Inspectorate is conducting in the performance of its functions under the Victorian Inspectorate Act; or
- (d) in the case of the Crime and Corruption Commission—means an investigation that the Commission is conducting in the

performance of its functions under the Crime and Corruption Act; or

- (f) in the case of the Law Enforcement Conduct Commission—means an investigation that the Commission is conducting in the performance of its functions under the *Law Enforcement Conduct Commission Act 2016* (NSW); or
- (fa) in the case of the Inspector of the Law Enforcement Conduct Commission—means an investigation that the Inspector is conducting in the performance of the Inspector’s functions under the *Law Enforcement Conduct Commission Act 2016* (NSW); or
- (i) in the case of the Corruption and Crime Commission—means an investigation that the Commission is conducting in the performance of its functions under the Corruption and Crime Commission Act; or
- (j) in the case of the Parliamentary Inspector of the Corruption and Crime Commission—means dealing with a matter of misconduct in the performance of the Parliamentary Inspector’s functions under the Corruption and Crime Commission Act; or
- (k) in the case of the Independent Commissioner Against Corruption—means an investigation that the Independent Commissioner Against Corruption is conducting in the performance of the Commissioner’s functions under the Independent Commissioner Against Corruption Act.

prescribed offence means:

- (a) a serious offence, or an offence that was a serious offence when the offence was committed;
- (b) an offence against subsection 7(1) or section 63; or
- (ba) an offence against subsection 108(1) or section 133; or
- (c) an offence against a provision of Part 10.6 of the *Criminal Code*; or
- (d) any other offence punishable by imprisonment for life or for a period, or maximum period, of at least 3 years; or
- (e) an ancillary offence relating to an offence of a kind referred to in paragraph (a), (b), (c) or (d) of this definition.

Section 5

prescribed substance means:

- (a) a substance that is a narcotic drug or psychotropic substance for the purposes of the *Crimes (Traffic in Narcotic Drugs and Psychotropic Substances) Act 1990*; or
- (b) a controlled drug or border controlled drug within the meaning of Part 9.1 of the *Criminal Code*; or
- (c) a controlled plant or border controlled plant within the meaning of Part 9.1 of the *Criminal Code*; or
- (d) a controlled precursor or border controlled precursor within the meaning of Part 9.1 of the *Criminal Code*.

preservation notice means a domestic preservation notice or a foreign preservation notice.

preservation notice information has the meaning given by section 6EAA.

preserve, in relation to a stored communication, means maintain the integrity of:

- (a) the stored communication; or
- (b) a copy of the stored communication.

preventative detention order law means:

- (a) Division 105 of the *Criminal Code*; or
- (b) Part 2A of the *Terrorism (Police Powers) Act 2002* (NSW); or
- (c) Part 2A of the *Terrorism (Community Protection) Act 2003* (Vic.); or
- (d) the *Terrorism (Preventative Detention) Act 2005* (Qld); or
- (e) the *Terrorism (Preventative Detention) Act 2006* (WA); or
- (f) the *Terrorism (Preventative Detention) Act 2005* (SA); or
- (g) the *Terrorism (Preventative Detention) Act 2005* (Tas.); or
- (h) Part 2 of the *Terrorism (Extraordinary Temporary Powers) Act 2006* (ACT); or
- (i) Part 2B of the *Terrorism (Emergency Powers) Act* (NT).

Note: For when a purpose is connected with a preventative detention order law, see the definition of **connected with**.

proceeding means:

- (a) a proceeding or proposed proceeding in a federal court or in a court of a State or Territory;
- (b) a proceeding or proposed proceeding, or a hearing or proposed hearing, before a tribunal in Australia, or before any other body, authority or person in Australia having power to hear or examine evidence; or
- (c) an examination or proposed examination by or before such a tribunal, body, authority or person.

Public Interest Advocate means a person declared under section 180X to be a Public Interest Advocate.

publicly-listed ASIO number has the meaning given by subsection 6(3).

record (except when used in Schedule 1) means:

- (a) in relation to information—a record or copy, whether in writing or otherwise, of the whole or a part of the information; or
- (b) in relation to an interception, whether or not in contravention of subsection 7(1), of a communication:
 - (i) a record or copy, whether in writing or otherwise, of the whole or a part of the communication, being a record or copy made by means of the interception; or
 - (ii) a record or copy, whether in writing or otherwise, of the whole or a part of a record or copy that is, by virtue of any other application or applications of this definition, a record obtained by the interception.

related account, service or device, in relation to a service to which Part 5-1A applies, means:

- (a) an account; or
- (b) a telecommunications device; or
- (c) another service of a kind referred to in paragraph 187A(3)(a); that is related to the service.

Section 5

relates:

- (a) a stored communication ***relates*** to a person only if it is:
 - (i) a stored communication that the person has made; or
 - (ii) a stored communication that another person has made and for which the person is the intended recipient; and
- (b) a stored communication ***relates*** to a telecommunications service only if it has passed over a telecommunications system by way of the telecommunications service.

relevant offence, in relation to a Commonwealth agency, an eligible Commonwealth authority or an eligible authority of a State, means:

- (a) in the case of the Australian Federal Police—a prescribed offence that is an offence against a law of the Commonwealth; or
- (aa) in the case of the Australian Commission for Law Enforcement Integrity—a prescribed investigation concerning conduct that involves a prescribed offence or possible conduct that would involve a prescribed offence; or
- (b) in the case of the ACC—a prescribed offence to which a prescribed investigation relates; or
- (ba) in the case of an eligible Commonwealth authority—a prescribed offence to which a prescribed investigation relates; or
- (c) in the case of the Police Force of a State—a prescribed offence that is an offence against a law of that State; or
- (d) in the case of the Crime Commission—a prescribed offence that is an offence against a law of New South Wales and to which a prescribed investigation relates; or
- (e) in the case of the Independent Commission Against Corruption—a prescribed offence that is an offence against a law of New South Wales and to which a prescribed investigation relates; or
- (ea) in the case of the Inspector of the Independent Commission Against Corruption—a prescribed offence that is an offence

- against a law of New South Wales and to which a prescribed investigation relates; or
- (eb) in the case of the IBAC—a prescribed offence that is an offence against a law of Victoria and to which a prescribed investigation relates; or
 - (ec) in the case of the Victorian Inspectorate—a prescribed offence that is an offence against the law of Victoria and to which a prescribed investigation relates; or
 - (f) in the case of the Crime and Corruption Commission—a prescribed offence that is an offence against the law of Queensland and to which a prescribed investigation relates; or
 - (h) in the case of the Law Enforcement Conduct Commission—a prescribed offence that is an offence against the law of New South Wales and to which a prescribed investigation relates; or
 - (ha) in the case of the Inspector of the Law Enforcement Conduct Commission—a prescribed offence that is an offence against a law of New South Wales and to which a prescribed investigation relates; or
 - (k) in the case of the Corruption and Crime Commission—a prescribed offence that is an offence against the law of Western Australia and to which a prescribed investigation relates; or
 - (l) in the case of the Parliamentary Inspector of the Corruption and Crime Commission—a prescribed offence that is an offence against the law of Western Australia and to which a prescribed investigation relates; or
 - (m) in the case of the Independent Commissioner Against Corruption—a prescribed offence that is an offence against the law of South Australia and to which a prescribed investigation relates.

relevant period, for a domestic preservation notice, means:

- (a) for an historic domestic preservation notice—the period referred to in subparagraph 107H(1)(b)(i); and

Section 5

- (b) for an ongoing domestic preservation notice—the period referred to in subparagraph 107H(1)(b)(ii).

relevant staff member of an enforcement agency means:

- (a) the head (however described) of the enforcement agency; or
- (b) a deputy head (however described) of the enforcement agency; or
- (c) any employee, member of staff or officer of the enforcement agency.

relevant statistics, in relation to applications of a particular kind, (except when used in Schedule 1) means all of the following:

- (a) how many applications of that kind were made;
- (b) how many applications of that kind were withdrawn or refused; and
- (c) how many warrants were issued on applications of that kind.

renewal, in relation to a warrant issued to an agency in respect of a telecommunications service or person, means a warrant:

- (a) that is issued to the agency in respect of that service or person; and
 - (b) the application for which was made while:
 - (i) the first-mentioned warrant; or
 - (ii) a warrant that is, by virtue of any other application or applications of this definition, a renewal of the first-mentioned warrant;
- was still in force.

renewal application means an application by an agency for a warrant in respect of a telecommunications service or person, being an application made while a warrant issued to the agency in respect of that service or person is still in force.

responsible person for a computer network means:

- (a) if an individual operates the network, or the network is operated on behalf of an individual—that individual; or

- (b) if a body (whether or not a body corporate) operates the network, or the network is operated on behalf of a body (whether or not a body corporate):
- (i) the head (however described) of the body, or a person acting as that head; or
 - (ii) if one or more positions are nominated by that head, or the person acting as that head, for the purposes of this subparagraph—each person who holds, or is acting in, such a position.

restricted record means a record other than a copy, that was obtained by means of an interception, whether or not in contravention of subsection 7(1), of a communication passing over a telecommunications system, but does not include a record of general computer access intercept information, a record of data disruption intercept information or a record of network activity warrant intercept information.

retained data means information, or documents, that a service provider is or has been required to keep under Part 5-1A.

satellite-based facility means a facility in a satellite.

secretary has the same meaning as in the *Corporations Act 2001*.

security has the same meaning as it has in the *Australian Security Intelligence Organisation Act 1979*.

security authority means an authority of the Commonwealth that has functions primarily relating to:

- (a) security; or
- (b) collection of foreign intelligence; or
- (c) the defence of Australia; or
- (d) the conduct of the Commonwealth's international affairs.

senior executive AFP employee has the same meaning as in the *Australian Federal Police Act 1979*.

serious contravention has the meaning given by section 5E.

Section 5

serious foreign contravention means:

- (a) a contravention of a law of a foreign country that is punishable by a maximum penalty of:
 - (i) imprisonment for 3 years or more, imprisonment for life or the death penalty; or
 - (ii) a fine of an amount that is at least equivalent to 900 penalty units; or
- (b) a crime within the jurisdiction of the ICC; or
- (c) a War Crimes Tribunal offence.

serious offence has the meaning given by section 5D.

serious Part 5.3 offence has the meaning given by section 105A.2 of the *Criminal Code*.

service provider has the meaning given by subsection 187A(1).

source (except in item 2 of the table in subsection 187AA(1)) means a person who provides information:

- (a) to another person who is working in a professional capacity as a journalist; and
- (b) in the normal course of the other person's work in such a capacity; and
- (c) in the expectation that the information may be disseminated in the form of:
 - (i) news, current affairs or a documentary; or
 - (ii) commentary or opinion on, or analysis of, news, current affairs or a documentary.

special ACC investigation has the same meaning as in the ACC Act.

special ACC operation/investigation has the same meaning as in the ACC Act.

special investigation means an investigation into matters relating to federally relevant criminal activity that the ACC is conducting

and that the Board of the ACC has determined to be a special investigation.

Special Register means the Special Register of Warrants kept under section 81C.

staff member, in relation to the Australian Federal Police, means an AFP employee who is not a member of the Australian Federal Police.

staff member of ACLEI has the same meaning as in the *Law Enforcement Integrity Commissioner Act 2006*.

staff member of ASIC has the same meaning as **staff member** in the *Australian Securities and Investments Commission Act 2001*.

State includes the Northern Territory.

stored communication (except when used in Schedule 1) means a communication that:

- (a) is not passing over a telecommunications system; and
- (b) is held on equipment that is operated by, and is in the possession of, a carrier; and
- (c) cannot be accessed on that equipment, by a person who is not a party to the communication, without the assistance of an employee of the carrier.

stored communications warrant means a warrant issued under Chapter 3.

stored communications warrant information has the meaning given by section 6EB.

subscriber means a person who rents or uses a telecommunications service.

succeeding Part 5.3 supervisory order has the meaning given by section 6U.

Section 5

telecommunications device means a terminal device that is capable of being used for transmitting or receiving a communication over a telecommunications system.

telecommunications network means a system, or series of systems, for carrying communications by means of guided or unguided electromagnetic energy or both, but does not include a system, or series of systems, for carrying communications solely by means of radiocommunication. This definition does not apply to Schedule 1.

telecommunications number means the address used by a carrier for the purposes of directing a communication to its intended destination and identifying the origin of the communication, and includes:

- (a) a telephone number; and
- (b) a mobile telephone number; and
- (c) a unique identifier for a telecommunications device (for example, an electronic serial number or a Media Access Control address); and
- (d) a user account identifier; and
- (e) an internet protocol address; and
- (f) an email address.

telecommunications service means a service for carrying communications by means of guided or unguided electromagnetic energy or both, being a service the use of which enables communications to be carried over a telecommunications system operated by a carrier but not being a service for carrying communications solely by means of radiocommunication.

telecommunications service warrant means an interception warrant issued or to be issued under section 9, 11A, 46 or 48.

telecommunications system means:

- (a) a telecommunications network that is within Australia; or
- (b) a telecommunications network that is partly within Australia, but only to the extent that the network is within Australia;

and includes equipment, a line or other facility that is connected to such a network and is within Australia.

telephone application (except when used in Schedule 1) means an application made by telephone for a Part 2-5 warrant or a stored communications warrant.

Territory does not include the Northern Territory.

terrorist act has the same meaning as in Part 5.3 of the *Criminal Code*.

terrorist offender has the meaning given by section 105A.2 of the *Criminal Code*.

unexplained wealth legislation has the same meaning as in the *Proceeds of Crime Act 2002*.

Victorian Inspectorate means the Victorian Inspectorate established under the Victorian Inspectorate Act.

Victorian Inspectorate Act means the *Victorian Inspectorate Act 2011* of Victoria.

Victorian Inspectorate officer means a person who is a Victorian Inspectorate Officer (within the meaning of the Victorian Inspectorate Act).

War Crimes Tribunal has the same meaning as **Tribunal** in the *International War Crimes Tribunals Act 1995*.

War Crimes Tribunal offence has the same meaning as **Tribunal offence** in the *International War Crimes Tribunals Act 1995*.

warrant means:

- (a) except in Chapter 2—an interception warrant or a stored communications warrant; or
- (b) in Chapter 2 (except in Part 2-5)—an interception warrant (whether issued before or after the commencement of this definition), a general computer access warrant, a data

Section 5

disruption warrant, a network activity warrant or an ASIO computer access warrant; or

(c) in Part 2-5—a Part 2-5 warrant.

working day means any day except:

(a) a Saturday or a Sunday; or

(b) a day that is a public holiday in any State or Territory.

(2) Where a telecommunications service is provided by a carrier for the use of an employee or employees of the carrier (not being a telecommunications service to which that person is the subscriber or those persons are subscribers), the carrier shall, for the purposes of this Act, be deemed to be the subscriber to that telecommunications service.

(3) For the purposes of this Act, the question whether equipment, or a line or other facility, is connected to a telecommunications network is to be determined in the same manner as that question is determined for the purposes of the *Telecommunications Act 1997*.

(4) A reference in this Act to the Attorney-General shall, at a time when the Attorney-General is absent from Australia or when, by reason of illness of the Attorney-General or for any other reason, the Director-General of Security cannot readily communicate with the Attorney-General, be read as including a reference to a Minister who has been authorized in writing by the Attorney-General to perform the functions of the Attorney-General under this Act at such a time.

(4A) A reference in this Act to an employee of a carrier includes a reference to a person who is engaged by the carrier or whose services are made available to the carrier.

(4B) A reference in this Act to an employee of a security authority includes a reference to a person who is engaged by the security authority or whose services are made available to the security authority.

(5) For the purposes of the definition of **telecommunications system** in subsection (1), a telecommunications network shall be taken to be

within Australia to the extent that the network is used for the purpose of carrying communications:

- (a) over an earth-based facility within Australia, or between earth-based facilities within Australia;
- (b) from an earth-based facility within Australia to a satellite-based facility, but only to the extent that the next earth-based facility to which the communications will be carried is an earth-based facility within Australia;
- (c) from a satellite-based facility to an earth-based facility within Australia, but only to the extent that the last earth-based facility from which the communications were carried was an earth-based facility within Australia; and
- (d) over a satellite-based facility, or between satellite-based facilities, but only to the extent that:
 - (i) the last earth-based facility from which the communications were carried was an earth-based facility within Australia; and
 - (ii) the next earth-based facility to which the communications will be carried is an earth-based facility within Australia;

whether or not the communications originated in Australia, and whether or not the final destination of the communications is within Australia.

- (6) For the purposes of the definition of *foreign intelligence* in subsection (1), *Australia* includes the external Territories.

Permitted purposes—Inspector of the Law Enforcement Conduct Commission

- (6A) For the purposes of subparagraph (dc)(i) of the definition of *permitted purpose* in subsection (1), *agency maladministration* in relation to the Law Enforcement Conduct Commission has the same meaning as it has in the *Law Enforcement Conduct Commission Act 2016* (NSW) in relation to the NSW Police Force or the Crime Commission.

Section 5AA

Permitted purposes—Law Enforcement Conduct Commission

- (7) For the purposes of subparagraph (e)(i) of the definition of ***permitted purpose*** in subsection (1), this subsection applies to conduct that:
- (a) both:
 - (i) involves a police officer, administrative employee or Crime Commission officer; and
 - (ii) the Law Enforcement Conduct Commission has decided is (or could be) serious misconduct or officer maladministration that is serious maladministration and should be investigated; or
 - (b) both:
 - (i) involves the Commissioner of Police or a Deputy Commissioner of Police; and
 - (ii) is (or could be) police misconduct or officer maladministration; or
 - (c) both:
 - (i) involves the Crime Commissioner or an Assistant Commissioner of the Crime Commission; and
 - (ii) is (or could be) Crime Commission officer misconduct or officer maladministration; or
 - (d) both Houses of the Parliament of New South Wales refer to the Commission for investigation under section 196 of the *Law Enforcement Conduct Commission Act 2016* (NSW).
- (8) An expression used in subsection (7) of this section and in the *Law Enforcement Conduct Commission Act 2016* (NSW) has the same meaning in that subsection as in that Act.

5AA Eligible Commonwealth authority declarations

The Minister may, by notice published in the *Gazette*, declare a Commonwealth Royal Commission to be an eligible Commonwealth authority for the purposes of this Act if the Minister is satisfied that the Royal Commission is likely to inquire

into matters that may involve the commission of a prescribed offence.

5AB Authorised officers

Authorised officers of an enforcement agency

- (1) The head (however described) of an enforcement agency may, by writing, authorise a management office or management position in the enforcement agency for the purposes of subparagraph (b)(iii) of the definition of **authorised officer** in subsection 5(1).

Authorised officers of the Australian Federal Police

- (1A) The Commissioner of Police may authorise, in writing, a senior executive AFP employee who is a member of the Australian Federal Police to be an authorised officer.
- (2) A copy of an authorisation must be given to the Communications Access Coordinator:
 - (a) in the case of an authorisation made under subsection (1)—by the head of the enforcement agency; and
 - (b) in the case of an authorisation made under subsection (1A)—by the Commissioner of Police.

Authorisations are not legislative instruments

- (3) An authorisation made under this section is not a legislative instrument.

5AC Authorisation of certifying officers

- (1) The Commissioner of Police may authorise, in writing, a senior executive AFP employee who is a member of the Australian Federal Police to be a certifying officer of the Australian Federal Police.

Section 5AC

- (2) The Integrity Commissioner may authorise, in writing, a staff member of ACLEI who is an SES employee to be a certifying officer of ACLEI.
- (3) The Chief Executive Officer of the ACC may authorise, in writing, a member of the staff of the ACC who is an SES employee or acting SES employee to be a certifying officer of the ACC.
- (4) The Commissioner of a Police Force of a State may authorise, in writing, an officer of the police force of the State whose rank is equivalent to that of a senior executive AFP employee who is a member of the Australian Federal Police to be a certifying officer of the Police Force of the State.
- (5) The Commissioner of the Crime Commission may authorise, in writing, a member of the staff of the Crime Commission who occupies an office or position at an equivalent level to that of a Public Service senior executive (within the meaning of the *Government Sector Employment Act 2013* (NSW)) to be a certifying officer of the Crime Commission.
- (6) The Chief Commissioner of the Independent Commission Against Corruption may authorise, in writing, an officer of the Independent Commission Against Corruption who occupies an office or position at an equivalent level to that of a Public Service senior executive (within the meaning of the *Government Sector Employment Act 2013* (NSW)) to be a certifying officer of the Independent Commission Against Corruption.
- (7) The Commissioner of the IBAC may authorise, in writing, an IBAC officer who occupies an office or position at an equivalent level to that of an executive (within the meaning of the *Public Administration Act 2004* of Victoria) to be a certifying officer of the IBAC.
- (8) The Chief Commissioner of the Law Enforcement Conduct Commission may authorise, in writing:
 - (a) an Assistant Commissioner of the Commission; or

Section 5AD

- (b) a member of the staff of the Law Enforcement Conduct Commission who occupies an office or position at an equivalent level to that of a Public Service senior executive (within the meaning of the *Government Sector Employment Act 2013* (NSW));
to be a certifying officer of the Commission.
- (9) The Commissioner of the Corruption and Crime Commission may authorise, in writing, an officer of the Corruption and Crime Commission who occupies an office or position at an equivalent level to that of a senior executive officer within the meaning of the *Public Sector Management Act 1994* of Western Australia to be a certifying officer of the Corruption and Crime Commission.
- (9A) The Independent Commissioner Against Corruption may authorise, in writing, a member of the staff of the Independent Commissioner Against Corruption who occupies an office or position at an equivalent level to that of an executive employee (within the meaning of the *Public Sector Act 2009* of South Australia) to be a certifying officer of the Independent Commissioner Against Corruption.
- (10) The chief executive officer of any other agency may authorise, in writing, an officer of the agency (by whatever name called) who holds, or is acting in, an office or position in the agency which is involved in the management of the agency to be a certifying officer of the agency.

5AD Authorisation of certifying person

The Director-General of Security may authorise, in writing, a senior position-holder (within the meaning of the *Australian Security Intelligence Organisation Act 1979*) to be a certifying person.

Section 5AE

**5AE Authorisation of members of the staff of a Commonwealth
Royal Commission**

A sole Commissioner or a member of a Commonwealth Royal Commission may authorise, in writing, a person assisting the Commission to be a member of the staff of the Commission for the purposes of this Act.

5A Communicating etc. certain information

For the purposes of this Act (other than Schedule 1), a person who gives to another person, makes use of, makes a record of, or produces in evidence in a proceeding, a record (in this section called the *relevant record*) obtained by an interception, whether or not in contravention of subsection 7(1), of a communication shall be taken to communicate to the other person, make use of, make a record of, or give in evidence in that proceeding, as the case may be, so much of the information obtained by the interception as can be derived from the relevant record.

5B Exempt proceedings

- (1) A reference in this Act to an exempt proceeding is a reference to:
- (a) a proceeding by way of a prosecution for a prescribed offence; or
 - (b) a proceeding for the confiscation or forfeiture of property, or for the imposition of a pecuniary penalty, in connection with the commission of a prescribed offence; or
 - (ba) a proceeding under the *Spam Act 2003*; or
 - (bb) a proceeding under, or a proceeding relating to a matter arising under, Division 104 (control orders) or Division 105A (post-sentence orders) of the *Criminal Code*; or
 - (bc) a proceeding under, or a proceeding relating to a matter arising under, a preventative detention order law, so far as the proceeding relates to a preventative detention order (within the meaning of that law); or

Section 5B

- (bd) a proceeding under, or a proceeding relating to a matter arising under, a post-sentence detention law or a post-sentence supervision law; or
- (be) a proceeding under, or a proceeding relating to a matter arising under, the main unexplained wealth provisions; or
- (bf) a proceeding under, or a proceeding relating to a matter arising under, the unexplained wealth legislation of a participating State, the Australian Capital Territory or the Northern Territory; or
- (c) a proceeding for the taking of evidence pursuant to section 43 of the *Extradition Act 1988*, in so far as the proceeding relates to a prescribed offence; or
- (ca) a proceeding under, or a proceeding relating to a matter arising under, an organised crime control law; or
- (d) a proceeding for the extradition of a person from a State or Territory to another State or Territory, in so far as the proceeding relates to a prescribed offence; or
- (da) a proceeding by way of a coroner's inquest if, in the opinion of the coroner, the event that is the subject of the inquest may have resulted from the commission of a prescribed offence; or
- (e) a police disciplinary proceeding; or
- (ea) a proceeding in so far as it relates to:
 - (i) a decision by the Commissioner of Police to terminate the employment of an AFP employee or the appointment of a special member of the Australian Federal Police; or
 - (ii) a decision by the Commissioner of a Police Force of a State to terminate the appointment of an officer or member of staff of that Police Force; or
- (eb) a proceeding in so far as it is, or relates to, disciplinary or legal action (within the meaning of section 6S) that is in relation to an eligible staff member (within the meaning of that section) of the Australian Federal Police or the ACC; or
- (f) any other proceeding (not being a proceeding by way of a prosecution for an offence) in so far as it relates to alleged

Section 5B

- misbehaviour, or alleged improper conduct, of an officer of the Commonwealth or of a State; or
- (g) a proceeding for the recovery of an amount due to a carrier in connection with the supply of a telecommunications service;
 - (h) a proceeding under section 13 of the *Mutual Assistance in Criminal Matters Act 1987* in relation to a criminal matter (within the meaning of that Act) that concerns an offence, against the laws of the foreign country that made the request resulting in the proceeding, that is punishable by imprisonment for life or for a period, or maximum period, of at least 3 years; or
 - (haa) a proceeding under Division 5 of Part 4 of the *International Criminal Court Act 2002*; or
 - (hab) a proceeding before the International Criminal Court sitting in Australia under Part 5 of the *International Criminal Court Act 2002*; or
 - (ha) a proceeding of an eligible Commonwealth authority; or
 - (hb) a proceeding of the Independent Commission Against Corruption; or
 - (hc) a proceeding of the Inspector of the Independent Commission Against Corruption; or
 - (hd) a proceeding in relation to an application under subsection 34B(1) of the *Australian Crime Commission Act 2002* in respect of contempt of the Australian Crime Commission; or
 - (i) a proceeding of the IBAC; or
 - (iaa) a proceeding of the Victorian Inspectorate; or
 - (ia) a proceeding of the Corruption and Crime Commission; or
 - (ib) a proceeding of the Parliamentary Inspector of the Corruption and Crime Commission; or
 - (j) a proceeding under Division 1 of Part 4 of the *International War Crimes Tribunals Act 1995*; or
 - (k) a proceeding of the Law Enforcement Conduct Commission; or
 - (ka) a proceeding of the Inspector of the Law Enforcement Conduct Commission; or
-

Section 5B

- (kb) a proceeding of the Crime and Corruption Commission; or
- (kc) a proceeding of the Independent Commissioner Against Corruption; or
- (l) a proceeding by way of a bail application if the application relates to a proceeding by way of a prosecution for a prescribed offence; or
- (m) a proceeding by way of review of a decision to refuse such a bail application; or
- (n) a proceeding by way of a review of a decision to grant such a bail application.

Note: Paragraphs (l), (m) and (n) were inserted as a response to the decision of the Court of Appeal of New South Wales in *Director of Public Prosecutions v Serratore* (1995) 132 ALR 461.

- (2) Without limiting subsection (1), a reference in Chapter 3 to an exempt proceeding includes a reference to:
 - (a) a proceeding by way of a prosecution for an offence punishable:
 - (i) by imprisonment for a period, or a maximum period, of at least 12 months; or
 - (ii) by a fine, or a maximum fine, of at least 60 penalty units if the offence is committed by an individual; or
 - (iii) if the offence cannot be committed by an individual—by a fine, or a maximum fine, of at least 300 penalty units; or
 - (b) a proceeding for the confiscation or forfeiture of property, or for the imposition of a pecuniary penalty, in connection with the commission of such an offence; or
 - (c) a proceeding for the taking of evidence pursuant to section 43 of the *Extradition Act 1988*, in so far as the proceeding relates to such an offence; or
 - (d) a proceeding for the extradition of a person from a State or Territory to another State or Territory, in so far as the proceeding relates to such an offence; or

Section 5C

- (e) a proceeding by way of a coroner's inquest if, in the opinion of the coroner, the event that is the subject of the inquest may have resulted from the commission of such an offence; or
- (f) a proceeding for recovery of a pecuniary penalty for a contravention that would, if proved, render the person committing the contravention liable to:
 - (i) a pecuniary penalty, or a maximum pecuniary penalty, of at least 60 penalty units if the contravention is committed by an individual; or
 - (ii) if the contravention cannot be committed by an individual—a pecuniary penalty, or a maximum pecuniary penalty, of at least 300 penalty units.

5C Information or question relevant to inspection by Ombudsman

- (1) For the purposes of this Act, information or a question is relevant to an inspection under Part 2-7 or Chapter 4A of an agency's records if the information or question is about:
 - (a) in any case:
 - (i) the location;
 - (ii) the making, compilation or keeping; or
 - (iii) the accuracy or completeness;of any of those records;
 - (b) in any case—any matter to which any of those records relates; or
 - (c) if the Ombudsman suspects on reasonable grounds that an officer of the agency has contravened this Act—any matter relating to the suspected contravention.
- (2) Nothing in subsection (1) limits the generality of a reference in this Act to information, or to a question, that is relevant to an inspection of an agency's records.

5D Serious offences

General types of serious offences

- (1) An offence is a **serious offence** if it is:
- (a) a murder, or an offence of a kind equivalent to murder; or
 - (b) a kidnapping, or an offence of a kind equivalent to kidnapping; or
 - (c) an offence against Division 307 of the *Criminal Code*; or
 - (d) an offence constituted by conduct involving an act or acts of terrorism; or
 - (e) an offence against:
 - (i) Subdivision A of Division 72 of the *Criminal Code*; or
 - (ia) Subdivision B of Division 80 of the *Criminal Code*; or
 - (ib) section 80.2C of the *Criminal Code*; or
 - (ic) Division 82 of the *Criminal Code* (sabotage); or
 - (id) Division 83 of the *Criminal Code* (other threats to security); or
 - (ie) Division 91 of the *Criminal Code* (espionage); or
 - (if) Division 92 of the *Criminal Code* (foreign interference); or
 - (ig) Division 92A of the *Criminal Code* (theft of trade secrets involving foreign government principal); or
 - (ii) Division 101 of the *Criminal Code*; or
 - (iii) Division 102 of the *Criminal Code*; or
 - (iv) Division 103 of the *Criminal Code*; or
 - (v) section 104.27 of the *Criminal Code*; or
 - (va) section 105A.18A of the *Criminal Code*; or
 - (vi) Division 119 of the *Criminal Code*; or
 - (vii) Division 122 of the *Criminal Code* (secrecy of information); or
 - (viii) section 137.1A of the *Criminal Code* (aggravated offence for giving false or misleading information); or

Section 5D

- (f) except for the purposes of an application for a warrant by an agency other than the ACC, an offence in relation to which the ACC is conducting an ACC special investigation.
- (2) An offence is also a *serious offence* if:
- (a) it is an offence punishable by imprisonment for life or for a period, or maximum period, of at least 7 years; and
 - (b) the particular conduct constituting the offence involved, involves or would involve, as the case requires:
 - (i) loss of a person's life or serious risk of loss of a person's life; or
 - (ii) serious personal injury or serious risk of serious personal injury; or
 - (iii) serious damage to property in circumstances endangering the safety of a person; or
 - (iiia) serious arson; or
 - (iv) trafficking in prescribed substances; or
 - (v) serious fraud; or
 - (vi) serious loss to the revenue of the Commonwealth, a State or the Australian Capital Territory; or
 - (vii) bribery or corruption of, or by:
 - (A) an officer of the Commonwealth; or
 - (B) an officer of a State; or
 - (C) an officer of a Territory; or

Offences involving planning and organisation

- (3) An offence is also a *serious offence* if it is an offence punishable by imprisonment for life or for a period, or maximum period, of at least 7 years, where the offence:
- (a) involves 2 or more offenders and substantial planning and organisation; and
 - (b) involves, or is of a kind that ordinarily involves, the use of sophisticated methods and techniques; and
 - (c) is committed, or is of a kind that is ordinarily committed, in conjunction with other offences of a like kind; and

- (d) consists of, or involves, any of the following:
- (i) theft;
 - (ii) handling of stolen goods;
 - (iii) tax evasion;
 - (iv) currency violations;
 - (v) extortion;
 - (vi) bribery or corruption of, or by:
 - (A) an officer of the Commonwealth; or
 - (B) an officer of a State; or
 - (C) an officer of a Territory;
 - (vii) bankruptcy violations;
 - (viii) company violations;
 - (ix) harbouring criminals;
 - (x) dealings in firearms or armaments;
 - (xi) a sexual offence against a person who is under 16;
 - (xii) an immigration offence.

Offences relating to criminal groups

- (3AA) An offence is also a **serious offence** if it is an offence against section 93T of the *Crimes Act 1900* of New South Wales.

Offences relating to people smuggling, slavery, sexual servitude, deceptive recruiting and trafficking in persons etc.

- (3A) An offence is also a **serious offence** if it is an offence against:
- (a) any of the following provisions of the *Criminal Code*:
 - (i) section 73.1, 73.2, 73.3, 73.3A, 73.8, 73.9, 73.10 or 73.11;
 - (ii) section 270.3, 270.5, 270.6A, 270.7, 270.7B or 270.7C (slavery or slavery-like offences);
 - (iii) section 271.2, 271.3, 271.4, 271.5, 271.6 or 271.7 (trafficking in persons);
 - (iv) section 271.7B, 271.7C, 271.7D or 271.7E (organ trafficking);

Section 5D

- (v) section 271.7F or 271.7G (harbouring victims); or
- (b) section 233A, 233B, 233C, 233D, 233E, 234 or 234A of the *Migration Act 1958*.

Sexual offences against children and offences involving child abuse material or harm to children

- (3B) An offence is also a serious offence if:
- (a) it is an offence against Division 272, 273 or 273A, Subdivision B or C of Division 471, or Subdivision D or F of Division 474, of the *Criminal Code*; or
 - (b) the particular conduct constituting the offence otherwise involved, involves or would involve:
 - (i) the production, publication, possession, supply or sale of, or other dealing in, child abuse material (within the meaning of Part 10.6 of the *Criminal Code*); or
 - (ii) consenting to or procuring the employment of a child, or employing a child, in connection with such material.

Money laundering offences etc.

- (4) An offence is also a **serious offence** if it is an offence against any of the following provisions:
- (a) Part 10.2 of the *Criminal Code* (other than section 400.9);
 - (b) Part 4AC of the *Crimes Act 1900* of New South Wales;
 - (c) section 194, 195 or 195A of the **Crimes Act 1958** of Victoria;
 - (d) section 64 of the *Crimes (Confiscation of Profits) Act 1989* of Queensland;
 - (e) section 563A of *The Criminal Code* of Western Australia;
 - (f) section 138 of the *Criminal Law Consolidation Act 1935* of South Australia;
 - (g) section 67 of the *Crime (Confiscation of Profits) Act 1993* of Tasmania;
 - (h) section 74 of the *Proceeds of Crime Act 1991* of the Australian Capital Territory;

- (i) Division 3A of Part VII of Schedule I to the *Criminal Code Act* of the Northern Territory.

Cybercrime offences etc.

- (5) An offence is also a **serious offence** if it is an offence against any of the following provisions:
- (a) Part 10.7 of the *Criminal Code*;
 - (b) section 308C, 308D, 308E, 308F, 308G, 308H or 308I of the *Crimes Act 1900* of New South Wales;
 - (c) section 247B, 247C, 247D, 247E, 247F, 247G or 247H of the **Crimes Act 1958** of Victoria;
 - (d) a provision of a law of a State (other than New South Wales or Victoria) that corresponds to a provision covered by paragraph (a), (b) or (c);
 - (e) a provision of a law of a Territory that corresponds to a provision covered by paragraph (a), (b) or (c);
 - (f) section 440A of *The Criminal Code* of Western Australia.

Serious drug offences

- (5A) An offence is also a **serious offence** if it is an offence against Part 9.1 of the *Criminal Code* (other than section 308.1 or 308.2).

Cartel offences

- (5B) An offence is also a **serious offence** if it is:
- (a) an offence against section 44ZZRF or 44ZZRG of the *Competition and Consumer Act 2010*; or
 - (b) an offence under subsection 79(1) of the *Competition and Consumer Act 2010* that relates to an offence covered by paragraph (a); or
 - (c) an offence against section 44ZZRF or 44ZZRG of the text set out in Part 1 of Schedule 1 to the *Competition and Consumer Act 2010*, so far as that section applies as a law of a State, the Northern Territory or the Australian Capital Territory; or

Section 5D

- (d) an offence under subsection 79(1) of the *Competition and Consumer Act 2010* (so far as that subsection applies as a law of a State, the Northern Territory or the Australian Capital Territory) that relates to an offence covered by paragraph (c).

Note: Offences covered by paragraph (c) or (d) form part of the Competition Code of the State or Territory concerned.

Market misconduct

- (5C) An offence is also a **serious offence** if it is an offence against any of the following provisions of the *Corporations Act 2001*:
- (a) section 1041A;
 - (b) subsection 1041B(1);
 - (c) subsection 1041C(1);
 - (d) section 1041D;
 - (e) subsection 1041E(1);
 - (f) subsection 1041F(1);
 - (g) section 1041G;
 - (h) subsection 1043A(1);
 - (i) subsection 1043A(2).

Offences connected with other serious offences

- (6) An offence is also a **serious offence** if it is an offence constituted by:
- (a) aiding, abetting, counselling or procuring the commission of;
or
 - (b) being, by act or omission, in any way, directly or indirectly, knowingly concerned in, or party to, the commission of; or
 - (c) conspiring to commit;
- an offence that is a serious offence under any of the preceding subsections.
- (7) An offence is also a **serious offence** if it is an offence constituted by receiving or assisting a person who is, to the offender's knowledge, guilty of a serious offence mentioned in subsection (1),

in order to enable the person to escape punishment or to dispose of the proceeds of the offence.

- (8) An offence is also a **serious offence** if it is an offence against any of the following provisions:
- (a) section 131.1, 135.1, 142.1 or 142.2, subsection 148.2(3), or section 268.112 of the *Criminal Code*;
 - (b) section 35, 36, 36A, 37, 39, 41, 42, 43, 46, 46A or 47 of the *Crimes Act 1914*.

Offences relating to criminal associations and organisations

- (8A) An offence is also a **serious offence** if it is an offence against Division 390 of the *Criminal Code*.

Offences relating to criminal organisations

- (9) An offence is also a **serious offence** if:
- (a) the particular conduct constituting the offence involved, involves or would involve, as the case requires:
 - (i) associating with a criminal organisation, or a member of a criminal organisation; or
 - (ii) contributing to the activities of a criminal organisation; or
 - (iii) aiding, abetting, counselling or procuring the commission of a prescribed offence for a criminal organisation; or
 - (iv) being, by act or omission, in any way, directly or indirectly, knowingly concerned in, or party to, the commission of a prescribed offence for a criminal organisation; or
 - (v) conspiring to commit a prescribed offence for a criminal organisation; and
 - (b) if the offence is covered by subparagraph (a)(i)—the conduct constituting the offence was engaged in, or is reasonably suspected of having been engaged in, for the purpose of supporting the commission of one or more prescribed offences by the organisation or its members; and

Section 5E

- (c) if the offence is covered by subparagraph (a)(ii)—the conduct constituting the offence was engaged in, or is reasonably suspected of having been engaged in, for the purpose of enhancing the ability of the organisation or its members to commit or facilitate the commission of one or more prescribed offences.

5E Serious contraventions

- (1) For the purposes of this Act, a *serious contravention* is a contravention of a law of the Commonwealth, a State or a Territory that:
 - (a) is a serious offence; or
 - (b) is an offence punishable:
 - (i) by imprisonment for a period, or a maximum period, of at least 3 years; or
 - (ii) if the offence is committed by an individual—by a fine, or a maximum fine, of at least 180 penalty units; or
 - (iii) if the offence cannot be committed by an individual—by a fine, or a maximum fine, of at least 900 penalty units; or
 - (c) could, if established, render the person committing the contravention liable:
 - (i) if the contravention were committed by an individual—to pay a pecuniary penalty of 180 penalty units or more, or to pay an amount that is the monetary equivalent of 180 penalty units or more; or
 - (ii) if the contravention cannot be committed by an individual—to pay a pecuniary penalty of 900 penalty units or more, or to pay an amount that is the monetary equivalent of 900 penalty units or more.
- (2) Except so far as the contrary intention appears, a contravention, or a contravention of a particular kind, is taken, for the purposes of this Act, to be a contravention, or to be a contravention of that kind, as the case may be, that:
 - (a) has been committed or is being committed; or

- (b) is suspected on reasonable grounds of having been committed, of being committed or of being likely to be committed.
- (3) To avoid doubt, a reference in this section to a number of penalty units in relation to a contravention of a law of a State or a Territory includes a reference to an amount of a fine or pecuniary penalty that is equivalent, under section 4AA of the *Crimes Act 1914*, to that number of penalty units.

5F When a communication is passing over a telecommunications system

For the purposes of this Act (other than Schedule 1), a communication:

- (a) is taken to start passing over a telecommunications system when it is sent or transmitted by the person sending the communication; and
- (b) is taken to continue to pass over the system until it becomes accessible to the intended recipient of the communication.

5G The intended recipient of a communication

For the purposes of this Act (other than Schedule 1), the *intended recipient* of a communication is:

- (a) if the communication is addressed to an individual (either in the individual's own capacity or in the capacity of an employee or agent of another person)—the individual; or
- (b) if the communication is addressed to a person who is not an individual—the person; or
- (c) if the communication is not addressed to a person—the person who has, or whose employee or agent has, control over the telecommunications service to which the communication is sent.

Section 5H

5H When a communication is accessible to the intended recipient

- (1) For the purposes of this Act, a communication is *accessible* to its intended recipient if it:
 - (a) has been received by the telecommunications service provided to the intended recipient; or
 - (b) is under the control of the intended recipient; or
 - (c) has been delivered to the telecommunications service provided to the intended recipient.
- (2) Subsection (1) does not limit the circumstances in which a communication may be taken to be accessible to its intended recipient for the purposes of this Act.

6 Interception of a communication

- (1) For the purposes of this Act (other than Schedule 1), but subject to this section, interception of a communication passing over a telecommunications system consists of listening to or recording, by any means, such a communication in its passage over that telecommunications system without the knowledge of the person making the communication.

Communications to or from emergency service facilities

- (2A) An *emergency service facility* is premises that are declared by the Minister, by written instrument, to be an emergency service facility.
- (2B) The Minister may declare premises to be an emergency service facility if the Minister is satisfied that the premises are operated by:
 - (a) a police force or service of the Commonwealth, of a State or of the Australian Capital Territory; or
 - (b) a fire service of a State or of the Australian Capital Territory; or
 - (c) an ambulance service of a State or of the Australian Capital Territory; or

Section 6

- (d) a service for despatching, or referring matters for the attention of, a force or service referred to in paragraph (a), (b) or (c);
to enable that force or service, or another force or service, to deal with a request for assistance in an emergency.
- (2C) A declaration by the Minister under subsection (2B) is not a legislative instrument.
- (2D) If the Minister makes a declaration under subsection (2B), the Minister must, by legislative instrument, specify:
- (a) the name of the force or service operating the premises to which the declaration relates; and
 - (b) the geographical region in which those premises are located.
- (2E) If a House of the Parliament disallows, in accordance with section 42 of the *Legislation Act 2003*, a legislative instrument made under subsection (2D), the declaration to which the instrument relates is taken to have been revoked at the time of the disallowance.
- (2F) If a person who is lawfully engaged in duties relating to the receiving and handling of communications to or from an emergency service facility listens to or records a communication passing over a telecommunications system to or from the emergency service facility, the listening or recording does not, for the purposes of this Act, constitute an interception of the communication.
- (2G) Subsection (2F) only applies in relation to an emergency service facility if signs notifying persons that communications to or from the facility may be listened to or recorded are clearly visible at each entrance to the facility.
- (2H) If:
- (a) an inspector under section 284 of the *Radiocommunications Act 1992* is lawfully engaged in performing spectrum management functions of the Australian Communications and Media Authority under the *Australian Communications*

Section 6

and Media Authority Act 2005 or the Radiocommunications Act 1992; and

- (b) while performing those spectrum management functions, the inspector incidentally listens to or records a communication passing over a telecommunications system;

the listening or recording does not, for the purposes of this Act, constitute an interception of the communication.

(2J) If:

- (a) an inspector under section 284 of the *Radiocommunications Act 1992* is lawfully engaged in exercising powers under Part 2 of the *Regulatory Powers (Standard Provisions) Act 2014* as it applies in relation to:

- (i) a provision mentioned in subsection 284A(1) of the *Radiocommunications Act 1992*; or
(ii) information mentioned in subsection 284A(2) of the *Radiocommunications Act 1992*; and

- (b) while exercising those powers, the inspector incidentally listens to or records a communication passing over a telecommunications system;

the listening or recording does not, for the purposes of this Act, constitute an interception of the communication.

(2K) If:

- (a) an inspector under section 284 of the *Radiocommunications Act 1992* is lawfully engaged in exercising powers under Part 3 of the *Regulatory Powers (Standard Provisions) Act 2014* as it applies in relation to a provision mentioned in subsection 284B(1) of the *Radiocommunications Act 1992*; and

- (b) while exercising those powers, the inspector incidentally listens to or records a communication passing over a telecommunications system;

the listening or recording does not, for the purposes of this Act, constitute an interception of the communication.

Section 6AAA

Communications to publicly-listed ASIO numbers

- (3) A **publicly-listed ASIO number** is a telephone number that:
- (a) enables members of the public to contact the Organisation; and
 - (b) is listed in:
 - (i) a telephone directory; or
 - (ii) a telephone number database; that is available to the public.
- (4) If:
- (a) a person makes a call to a publicly-listed ASIO number; and
 - (b) another person who is lawfully engaged in duties relating to the receiving and handling of communications to that number listens to or records a communication passing over a telecommunications system in the course of that call; the listening or recording does not, for the purposes of this Act, constitute the interception of the communication.

6AAA When a computer network is appropriately used by an employee etc. of a Commonwealth agency etc.

For the purposes of this Act, if a computer network is operated by, or on behalf of, a Commonwealth agency, security authority or eligible authority of a State, the network is **appropriately used** by an employee, office holder or contractor of the agency or authority if:

- (a) the employee, office holder or contractor has undertaken, in writing, to use the network in accordance with any conditions specified, in writing, by the agency or authority; and
- (b) those conditions are reasonable; and
- (c) the employee, office holder or contractor complies with those conditions when using the network.

Section 6AA

6AA Accessing a stored communication

For the purposes of this Act, *accessing* a stored communication consists of listening to, reading or recording such a communication, by means of equipment operated by a carrier, without the knowledge of the intended recipient of the communication.

6A Investigation of an offence

- (1) A reference in this Act to the investigation by an agency, or by an eligible authority of a State, of an offence is a reference to:
 - (a) in the case of the Australian Federal Police—an investigation of that offence, in the course of the performance by the Australian Federal Police of its functions, by members of the Australian Federal Police;
 - (b) in the case of a Police Force of a State—an investigation of that offence, in the course of the performance by that Police Force of its functions, by officers of that Police Force; or
 - (c) in the case of the following eligible authorities or agencies, a prescribed investigation, in so far as it relates to that offence:
 - (ia) the Australian Commission for Law Enforcement Integrity;
 - (i) the ACC;
 - (ii) the Crime Commission;
 - (iii) the Crime and Corruption Commission;
 - (v) the Independent Commission Against Corruption;
 - (va) the Inspector of the Independent Commission Against Corruption;
 - (vi) the Law Enforcement Conduct Commission;
 - (vii) the Inspector of the Law Enforcement Conduct Commission;
 - (viii) the IBAC;
 - (ix) the Victorian Inspectorate;
 - (x) the Corruption and Crime Commission;

Section 6B

- (xi) the Parliamentary Inspector of the Corruption and Crime Commission;
 - (xii) the Independent Commissioner Against Corruption.
- (2) A reference in this Act to an investigation, in relation to an offence, is, in the case of an offence that is suspected on reasonable grounds of being likely to be committed, a reference to the investigation of the likely commission of that offence.

6B Involvement in an offence

For the purposes of this Act, a person shall be taken to be involved in an offence if, and only if, the person:

- (a) has committed, or is committing, the offence; or
- (b) is suspected on reasonable grounds of having committed, of committing, or of being likely to commit, the offence.

6C Issue of warrant to agency or eligible authority

For the purposes of this Act, a warrant issued on an application by an agency or an officer of an agency, or on an application by an eligible authority of a State, shall be taken to be issued to that agency or eligible authority, as the case may be.

6D Judges

- (1) In this Act, unless the contrary intention appears:

eligible Judge (except when used in Schedule 1) means a Judge in relation to whom a consent under subsection (2) and a declaration under subsection (3) are in force.

Judge means a person who is a Judge of a court created by the Parliament.

- (2) A Judge may by writing consent to be nominated by the Attorney-General under subsection (3).

Section 6DA

- (3) The Attorney-General may by writing declare Judges in relation to whom consents are in force under subsection (2) to be eligible Judges for the purposes of this Act (other than Schedule 1).
- (4) An eligible Judge has, in relation to the performance or exercise of a function or power conferred on an eligible Judge by this Act (other than Schedule 1), the same protection and immunity as a Justice of the High Court has in relation to proceedings in the High Court.

6DA Nominated AAT members

- (1) The Attorney-General may, by writing, nominate a person who holds one of the following appointments to the Administrative Appeals Tribunal to issue warrants under Part 2-5:
 - (a) Deputy President;
 - (b) senior member (of any level);
 - (c) member (of any level).
- (2) Despite subsection (1), the Attorney-General must not nominate a person who holds an appointment as a part-time senior member or a member of the Tribunal unless the person:
 - (a) is enrolled as a legal practitioner of the High Court, of another federal court or of the Supreme Court of a State or of the Australian Capital Territory; and
 - (b) has been so enrolled for not less than 5 years.
- (3) A nomination ceases to have effect if:
 - (a) the nominated AAT member ceases to hold an appointment of a kind set out in subsection (1); or
 - (b) the Attorney-General, by writing, withdraws the nomination.
- (4) A nominated AAT member has, in performing a function of or connected with, issuing a warrant under Part 2-5, the same protection and immunity as a Justice of the High Court has in relation to proceedings in the High Court.

6DB Issuing authorities

- (1) The Attorney-General may, by writing, appoint as an issuing authority:
 - (a) a person who is:
 - (i) a judge of a court created by the Parliament; or
 - (ii) a magistrate;
and in relation to whom a consent under subsection (2) is in force; or
 - (b) a person who:
 - (i) holds an appointment to the Administrative Appeals Tribunal as Deputy President, senior member (of any level) or member (of any level); and
 - (ii) is enrolled as a legal practitioner of a federal court or of the Supreme Court of a State or a Territory; and
 - (iii) has been enrolled for at least 5 years.
- (2) A person who is:
 - (a) a judge of a court created by the Parliament; or
 - (c) a magistrate;may, by writing, consent to be appointed by the Attorney-General under subsection (1).
- (3) A person's appointment ceases to have effect if:
 - (a) the person ceases to be a person whom the Attorney-General could appoint under this section; or
 - (b) the Attorney-General, by writing, revokes the appointment.
- (3A) An appointment under subsection (1) has no effect for the purposes of Schedule 1.
- (4) An issuing authority has, in relation to the performance or exercise of a function or power conferred on an issuing authority by this Act (other than Schedule 1), the same protection and immunity as a Justice of the High Court has in relation to proceedings in the High Court.

Section 6DC

6DC Part 4-1 issuing authorities

- (1) The Attorney-General may, by writing, appoint as a Part 4-1 issuing authority:
 - (a) a person who is:
 - (i) a judge of a court created by the Parliament; or
 - (iii) a magistrate;and in relation to whom a consent under subsection (2) is in force; or
 - (b) a person who:
 - (i) holds an appointment to the Administrative Appeals Tribunal as Deputy President, full-time senior member, part-time senior member or member; and
 - (ii) is enrolled as a legal practitioner of a federal court or of the Supreme Court of a State or a Territory; and
 - (iii) has been enrolled for at least 5 years.
- (2) A person who is:
 - (a) a judge of a court created by the Parliament; or
 - (b) a magistrate;may, by writing, consent to be appointed by the Attorney-General under subsection (1).
- (3) A person's appointment ceases to have effect if:
 - (a) the person ceases to be a person whom the Attorney-General could appoint under this section; or
 - (b) the Attorney-General, by writing, revokes the appointment.
- (4) A Part 4-1 issuing authority has, in relation to the performance or exercise of a function or power conferred on a Part 4-1 issuing authority by this Act, the same protection and immunity as a Justice of the High Court has in relation to proceedings in the High Court.

6E Lawfully intercepted information

- (1) Subject to subsections (2) and (3), a reference in this Act to lawfully intercepted information is a reference to information obtained (whether before or after the commencement of this section) by intercepting, otherwise than in contravention of subsection 7(1), a communication passing over a telecommunications system.
- (2) A reference in this Act to lawfully intercepted information that was originally obtained by an agency, or by an eligible authority of a State, is a reference to:
 - (a) information obtained, whether before or after the commencement of this section, by intercepting a communication under a warrant issued to the agency or authority; or
 - (b) information communicated to the agency or authority in accordance with section 65A or 63E.
- (3) A reference in this Act to lawfully intercepted information does not include a reference to information obtained in accordance with an international production order (within the meaning of Schedule 1).

6EA Interception warrant information

A reference in this Act to *interception warrant information* is a reference to:

- (a) information about any of the following:
 - (i) an application for an interception warrant;
 - (ii) the issue of an interception warrant;
 - (iii) the existence or non-existence of an interception warrant;
 - (iv) the expiry of an interception warrant; or
- (b) any other information that is likely to enable the identification of:
 - (i) the telecommunications service to which an interception warrant relates; or

Section 6EAA

- (ii) a person specified in an interception warrant as a person using or likely to use the telecommunications service to which the warrant relates.

6EAA Preservation notice information

A reference in this Act to *preservation notice information* is a reference to:

- (a) information about any of the following:
 - (i) the giving of a preservation notice;
 - (ii) for a foreign preservation notice—the making of a request under section 107P to preserve stored communications covered by the notice;
 - (iii) the existence or non-existence of a preservation notice;
 - (iv) the expiry of a preservation notice; or
- (b) any other information that is likely to enable the identification of:
 - (i) the person or telecommunications service specified in a preservation notice; or
 - (ii) the person or telecommunications service to which a preservation notice relates.

6EB Stored communications warrant information

A reference in this Act to *stored communications warrant information* is a reference to:

- (a) information about any of the following:
 - (i) an application for a stored communications warrant;
 - (ii) the issue of a stored communications warrant;
 - (iii) the existence or non-existence of a stored communications warrant;
 - (iv) the expiry of a stored communications warrant; or
- (b) any other information that is likely to enable the identification of:
 - (i) the telecommunications service to which a stored communications warrant relates; or

- (ii) a person specified in a stored communications warrant as a person using or likely to use the telecommunications service to which the warrant relates.

6F Offences

Except so far as the contrary intention appears, a reference in this Act to an offence, or to an offence of a particular kind, is a reference to an offence, or to an offence of that kind, as the case may be, that:

- (a) has been committed or is being committed; or
- (b) is suspected on reasonable grounds of having been committed, of being committed or of being likely to be committed.

6G Officer of the Commonwealth, of a State or of a Territory

- (1) A reference in this Act to an *officer* of the Commonwealth includes a reference to:
 - (a) a person holding, or acting in, an office (including a judicial office) or appointment, or employed, under a law of the Commonwealth;
 - (b) a person who is, or is a member of, an authority or body established for a public purpose by or under a law of the Commonwealth, or is an officer or employee of such an authority or body; and
 - (c) an officer of the Australian Capital Territory;but does not include a reference to an officer of the Northern Territory or of an external Territory.
- (2) A reference in this Act to an *officer* of a State includes a reference to:
 - (a) a person holding, or acting in, an office (including a judicial office) or appointment, or employed, under a law of the State; and

Section 6H

- (b) a person who is, or is a member of, an authority or body established for a public purpose by or under a law of the State, or is an officer or employee of such an authority or body.
- (3) A reference in this Act to an *officer* of a Territory includes a reference to:
 - (a) a person holding, or acting in, an office (including a judicial office) or appointment, or employed, under a law of the Territory; and
 - (b) a person who is, or is a member of, an authority or body established for a public purpose by or under a law of the Territory, or is an officer or employee of such an authority or body.

6H Person to whom application relates

For the purposes of this Act, an application by an agency to a Judge or nominated AAT member for a warrant relates to a particular person if, and only if, information has been, or is proposed to be, given to the Judge or nominated AAT member under Part 2-5, in connection with the application, in order to satisfy the Judge or nominated AAT member, in relation to the person, of the matters referred to in:

- (a) in the case of a warrant under section 48—paragraphs 46(1)(c) and (d), 46(4)(c), (d) and (e), or 46(7)(c) to (h), as the case requires; or
- (b) in the case of any other Part 2-5 warrant—paragraphs 46(1)(c) and (d), 46(4)(c), (d) and (e), 46(7)(c) to (h), 46A(1)(c) and (d), 46A(2A)(c), (d) and (e) or 46A(2C)(c) to (h), as the case requires; or
- (c) in the case of a stored communications warrant—subparagraph 116(1)(d)(i) or (ii), as the case requires.

6J Proceeding by way of a prosecution for an offence

A reference in this Act to a proceeding by way of a prosecution for an offence includes a reference to a proceeding with a view to the committal of a person for trial for the offence.

6K Proceeding for confiscation or forfeiture or for pecuniary penalty

A reference in this Act to a proceeding, or to a proceeding under a law of the Commonwealth, for the confiscation or forfeiture of property, or for the imposition of a pecuniary penalty, in connection with the commission of a prescribed offence includes a reference to:

- (a) a proceeding for the condemnation or recovery of a ship or aircraft, or of goods, seized under section 203 of the *Customs Act 1901* in connection with the commission of an offence against:
 - (i) subsection 50(7) or subsection 112(2BC) of the *Customs Act 1901*; or
 - (ii) Division 307 of the *Criminal Code*; and
- (b) a proceeding by way of an application for an order under subsection 243B(1) of the *Customs Act 1901*; and
- (c) a proceeding by way of an application for a restraining order, or an order that is ancillary to a restraining order, under a prescribed Act of the Commonwealth, a State or the Australian Capital Territory.

6L Relevant proceeding

- (1) A reference in this Act, in relation to an agency, or an eligible authority of a State, to a relevant proceeding is, in the case of the Australian Federal Police or a Police Force of a State, a reference to:
 - (a) a proceeding by way of a prosecution for a prescribed offence that is an offence against a law of the Commonwealth, or of that State, as the case may be; or

Section 6L

- (b) a proceeding under a law of the Commonwealth, or of that State, as the case may be, for the confiscation or forfeiture of property, or for the imposition of a pecuniary penalty, in connection with the commission of a prescribed offence; or
- (ba) in the case of the Australian Federal Police—a proceeding under, or a proceeding relating to a matter arising under:
 - (i) the main unexplained wealth provisions; or
 - (ii) the unexplained wealth legislation of a participating State, the Australian Capital Territory or the Northern Territory; or
- (bb) in the case of the Police Force of a participating State, the Australian Capital Territory or the Northern Territory—a proceeding under, or a proceeding relating to a matter arising under, the unexplained wealth legislation of that State or Territory; or
- (c) a proceeding for the taking of evidence as mentioned in paragraph 5B(1)(c), in so far as the proceeding relates to:
 - (i) a prescribed offence; or
 - (ii) a prescribed offence that is an offence against a law of that State;as the case may be; or
- (ca) a proceeding under, or in relation to a matter arising under, an organised crime control law of that State; or
- (d) a proceeding for the extradition of a person as mentioned in paragraph 5B(1)(d), in so far as the proceeding relates to a prescribed offence that is an offence against a law of the Commonwealth, or of that State, as the case may be; or
- (e) a police disciplinary proceeding that is a proceeding against a member of the Australian Federal Police, or of that Police Force, as the case may be; or
- (ea) in the case of the Australian Federal Police:
 - (i) a proceeding against an AFP employee in so far as the proceeding relates to a decision by the Commissioner of Police to terminate the employment of the employee; or
 - (ii) a proceeding against a special member of the Australian Federal Police in so far as the proceeding relates to a

Section 6L

- decision by the Commissioner of Police to terminate the appointment of the member; or
- (eb) in the case of a Police Force of a State—a proceeding against an officer or member of staff of that Police Force in so far as the proceeding relates to a decision by the Commissioner of that Police Force to terminate the appointment of the officer or member of staff; or
- (f) any other proceeding (not being a proceeding by way of a prosecution for an offence) in so far as it relates to alleged misbehaviour, or alleged improper conduct, of an officer of the Commonwealth, or of that State, as the case may be.
- (2) A reference in this Act, in relation to an agency, or an eligible authority of a State, to a relevant proceeding is:
- (a) in the case of the Australian Commission for Law Enforcement Integrity or the ACC—a reference to:
- (i) a proceeding by way of a prosecution for a prescribed offence to which a prescribed investigation relates or related; or
- (ii) a proceeding under a law of the Commonwealth or a State for the confiscation or forfeiture of property, or for the imposition of a pecuniary penalty, in connection with the commission of a prescribed offence to which a prescribed investigation relates or related; or
- (aa) in the case of the Crime Commission—a reference to:
- (i) a proceeding by way of a prosecution for a prescribed offence that is an offence against the law of New South Wales and to which a prescribed investigation relates or related; or
- (ii) a proceeding under a law of New South Wales for the confiscation or forfeiture of property, or for the imposition of a pecuniary penalty, in connection with the commission of a prescribed offence; or
- (b) in the case of the Independent Commission Against Corruption, the Inspector of the Independent Commission Against Corruption, the Law Enforcement Conduct Commission or the Inspector of the Law Enforcement

Section 6L

- Conduct Commission—a reference to a proceeding by way of a prosecution for a prescribed offence:
- (i) that is an offence against the law of New South Wales; and
 - (ii) to which a prescribed investigation relates or related; or
- (ba) in the case of the IBAC or the Victorian Inspectorate—a reference to a proceeding by way of a prosecution for a prescribed offence:
- (i) that is an offence against the law of Victoria; and
 - (ii) to which a prescribed investigation relates or related; or
- (c) in the case of the Crime and Corruption Commission—a reference to:
- (i) a proceeding by way of a prosecution for a prescribed offence that is an offence against the law of Queensland and to which a prescribed investigation relates or related; or
 - (ii) a proceeding under a law of Queensland for the confiscation or forfeiture of property, or for the imposition of a pecuniary penalty, in connection with the commission of a prescribed offence; or
- (d) in the case of the Corruption and Crime Commission or the Parliamentary Inspector of the Corruption and Crime Commission—a reference to a proceeding by way of a prosecution for a prescribed offence:
- (i) that is an offence against the law of Western Australia; and
 - (ii) to which a prescribed investigation relates or related; or
- (e) in the case of the Independent Commissioner Against Corruption—a reference to a proceeding by way of prosecution for a prescribed offence:
- (i) that is an offence against the law of South Australia; and
 - (ii) to which a prescribed investigation relates or related.
- (3) A reference in this Act, in relation to an agency that is an interception agency, to a relevant proceeding is a reference to a

proceeding under, or a proceeding relating to a matter arising under:

- (a) the main unexplained wealth provisions; or
- (b) the unexplained wealth legislation of a participating State, the Australian Capital Territory or the Northern Territory.

6M Terminating the appointment of an officer

A reference in this Act to terminating, because of misbehaviour or improper conduct, the appointment of an officer of the Commonwealth or a State includes a reference to removing the officer from office on the ground of misbehaviour or improper conduct.

6N Declaration of staff members of State Police Forces

- (1) This section applies to an agency that is the Police Force of a State.
- (2) The Minister may make a written declaration that members of an agency included in a specified class of members of the agency occupy positions corresponding to those of AFP employees who are not members of the Australian Federal Police.
- (3) Members included in the class of members of an agency specified in a declaration are referred to in this Act, in relation to the agency concerned, as staff members.

6P Identification of service

For the purposes of this Act (other than Schedule 1), a service may be identified by:

- (a) a number assigned to it from time to time; or
- (b) by any other unique identifying factor.

6Q Identification of telecommunications device

For the purposes of this Act, a telecommunications device may be identified by:

Section 6R

- (a) a unique telecommunications number assigned to it from time to time; or
- (b) any other unique identifying factor.

6R Communications Access Co-ordinator

- (1) In this Act:

Communications Access Co-ordinator means:

- (a) the Secretary of the Department; or
 - (b) if a person or body is covered by an instrument under subsection (2)—that person or body.
- (2) The Minister may, by legislative instrument, specify a person or body for the purposes of paragraph (b) of the definition of *Communications Access Co-ordinator* in subsection (1).
- (3) Unless the context otherwise requires, an act done by or in relation to the Communications Access Co-ordinator is taken to be an act done by or in relation to the Co-ordinator on behalf of all the interception agencies and all the enforcement agencies.

6S Permitted purposes—integrity purposes

- (1) For the purposes of paragraph (aaa) of the definition of *permitted purpose* in subsection 5(1), a purpose mentioned in column 2 of an item in the following table is a *permitted purpose* in relation to a Commonwealth agency, or the Immigration and Border Protection Department, as mentioned in column 1 of that item.

Permitted purposes—integrity purposes		
Item	Column 1—Commonwealth agency or Immigration and Border Protection Department	Column 2—Permitted purpose
1	(a) Australian Federal Police; or (b) ACC; or	A purpose connected with: (a) a decision about whether to apply for an integrity authority; or

Section 6S

Permitted purposes—integrity purposes

Item	Column 1—Commonwealth agency or Immigration and Border Protection Department	Column 2—Permitted purpose
	(c) Australian Commission for Law Enforcement Integrity; or (d) Immigration and Border Protection Department.	(b) designing, but not conducting, an integrity operation; or (c) an application for an integrity authority; or (d) granting an integrity authority.
2	(a) Australian Federal Police; or (b) ACC; or (c) Australian Commission for Law Enforcement Integrity.	A purpose connected with an application for any warrant, authorisation or order, under a law of the Commonwealth, that is made for the purposes of an integrity operation.
3	(a) Australian Federal Police; or (b) ACC.	A purpose connected with disciplinary or legal action in relation to an eligible staff member of that agency, if arising out of, or otherwise related to, an integrity operation.

Note: The *Commonwealth agencies* are the ACC, the Australian Federal Police and the Australian Commission for Law Enforcement Integrity (see subsection 5(1)).

(2) In this section:

disciplinary or legal action, in relation to an eligible staff member of the Australian Federal Police or the ACC, means any of the following:

- (a) action in respect of alleged misconduct of the staff member;
- (b) termination of the employment or appointment of the staff member;
- (c) a disciplinary proceeding (within the meaning of the *Law Enforcement Integrity Commissioner Act 2006*) in relation to the staff member, or a report of such a proceeding;
- (d) the investigation of an offence suspected to have been committed by the staff member;

Section 6T

- (e) a legal proceeding in relation to the staff member, or a report of such a proceeding.

Disciplinary or legal action also includes the consideration of whether an action or proceeding covered by this definition should be taken or brought.

eligible staff member, of the Australian Federal Police or the ACC, means a staff member of that agency within the meaning of the *Law Enforcement Integrity Commissioner Act 2006* (see section 10 of that Act).

6T When a Part 5.3 supervisory order is taken to be in force

For the purposes of this Act, a Part 5.3 supervisory order is taken to be in force in relation to a person if:

- (a) the order is a control order that has been made but has not yet come into force because:
 - (i) it has not been served on the person; or
 - (ii) the person is detained in custody in a prison (within the meaning of Part 5.3 of the *Criminal Code*); or
- (b) the order is an extended supervision order or an interim supervision order that has been made but the period specified in the order under paragraph 105A.7A(4)(d) or 105A.9A(7)(c) of the *Criminal Code* has not yet begun.

6U Succeeding Part 5.3 supervisory orders

- (1) If 2 or more successive control orders are made in relation to the same person, each later control order is a **succeeding Part 5.3 supervisory order** in relation to each earlier control order.

Note: If an interim control order is confirmed, the confirmed control order is a succeeding Part 5.3 supervisory order in relation to the interim control order (see the definition of **control order** in section 5).

- (2) If an interim supervision order is made in relation to a person, any later extended supervision order in relation to the person is a **succeeding Part 5.3 supervisory order** in relation to an earlier interim supervision order.

Section 6U

- (3) If 2 or more successive extended supervision orders or interim supervision orders are made in relation to the same person, each later extended supervision order or interim supervision order is a ***succeeding Part 5.3 supervisory order*** in relation to each earlier extended supervision order or interim supervision order.

Section 7

Chapter 2—Interception of telecommunications

Part 2-1—Prohibition on interception of telecommunications

7 Telecommunications not to be intercepted

- (1) A person shall not:
 - (a) intercept;
 - (b) authorize, suffer or permit another person to intercept; or
 - (c) do any act or thing that will enable him or her or another person to intercept;a communication passing over a telecommunications system.
- (2) Subsection (1) does not apply to or in relation to:
 - (a) an act or thing done by an employee of a carrier in the course of his or her duties for or in connection with:
 - (i) the installation of any line, or the installation of any equipment, used or intended for use in connection with a telecommunications service; or
 - (ii) the operation or maintenance of a telecommunications system; or
 - (iii) the identifying or tracing of any person who has contravened, or is suspected of having contravened or being likely to contravene, a provision of Part 10.6 of the *Criminal Code*;
where it is reasonably necessary for the employee to do that act or thing in order to perform those duties effectively; or
 - (aa) the interception of a communication by another person lawfully engaged in duties relating to the installation, connection or maintenance of equipment or a line, where it is reasonably necessary for the person to intercept the

- communication in order to perform those duties effectively;
or
- (aaa) the interception of a communication by a person if:
 - (i) the person is authorised, in writing, by a responsible person for a computer network to engage in network protection duties in relation to the network; and
 - (ii) it is reasonably necessary for the person to intercept the communication in order to perform those duties effectively; or
 - (ab) the interception of a communication by a person lawfully engaged in duties relating to the installation, connection or maintenance of equipment used, or to be used, for the interception of communications under warrants; or
 - (ac) the interception of a communication where the interception results from, or is incidental to, action taken by an ASIO employee, in the lawful performance of his or her duties, for the purpose of:
 - (i) discovering whether a listening device is being used at, or in relation to, a particular place; or
 - (ii) determining the location of a listening device; or
 - (ad) the interception of a communication where the interception results from, or is incidental to, action taken by an ASIO affiliate, in accordance with the contract, agreement or other arrangement under which the ASIO affiliate is performing functions or services for the Organisation, for the purpose of:
 - (i) discovering whether a listening device is being used at, or in relation to, a particular place; or
 - (ii) determining the location of a listening device; or
 - (b) the interception of a communication under a warrant; or
 - (ba) the interception of a communication under subsection 25A(4) or (8), 27A(1) or (3C), 27E(2) or 27E(6) of the *Australian Security Intelligence Organisation Act 1979*; or
 - (bb) the interception of a communication under subsection 27E(7), 27KE(9) or 27KP(8) of the *Surveillance Devices Act 2004*; or

Section 7

- (bc) an act or thing done in compliance with an international production order (within the meaning of Schedule 1); or
 - (c) the interception of a communication pursuant to a request made, or purporting to be made, under subsection 30(1) or (2); or
 - (d) the interception of a communication under an authorisation under section 31A.
- (2A) For the purposes of paragraphs (2)(a), (aa) and (aaa), in determining whether an act or thing done by a person was reasonably necessary in order for the person to perform his or her duties effectively, a court is to have regard to such matters (if any) as are specified in, or ascertained in accordance with, the regulations.
- (3) Paragraph (2)(aaa) does not apply to a voice communication in the form of speech (including a communication that involves a recorded or synthetic voice).
- (4) Subsection (1) does not apply to, or in relation to, an act done by an officer of an agency in relation to a communication if the following conditions are satisfied:
- (a) the officer or another officer of the agency is a party to the communication; and
 - (b) there are reasonable grounds for suspecting that another party to the communication has:
 - (i) done an act that has resulted, or may result, in loss of life or the infliction of serious personal injury; or
 - (ii) threatened to kill or seriously injure another person or to cause serious damage to property; or
 - (iii) threatened to take his or her own life or to do an act that would or may endanger his or her own life or create a serious threat to his or her health or safety; and
 - (c) because of the urgency of the need for the act to be done, it is not reasonably practicable for an application for a Part 2-5 warrant to be made.

- (5) Subsection (1) does not apply to, or in relation to, an act done by an officer of an agency in relation to a communication if the following conditions are satisfied:
- (a) the person to whom the communication is directed has consented to the doing of the act; and
 - (b) there are reasonable grounds for believing that that person is likely to receive a communication from a person who has:
 - (i) done an act that has resulted, or may result, in loss of life or the infliction of serious personal injury; or
 - (ii) threatened to kill or seriously injure another person or to cause serious damage to property; or
 - (iii) threatened to take his or her own life or to do an act that would or may endanger his or her own life or create a serious threat to his or her health or safety; and
 - (c) because of the urgency of the need for the act to be done, it is not reasonably practicable for an application for a Part 2-5 warrant to be made.
- (6) As soon as practicable after the doing of an act in relation to a communication under the provisions of subsection (4) or (5), an officer of the agency which is concerned with the communication shall cause an application for a Part 2-5 warrant to be made in relation to the matter.
- (6A) Subsection (6) does not apply if action has been taken under subsection (4) or (5) to intercept a communication, or cause it to be intercepted, and the action has ceased before it is practicable for an application for a Part 2-5 warrant to be made.
- (7) Where after considering an application made in relation to a matter arising under subsections (4) or (5) and (6) a Judge or nominated AAT member does not issue a warrant in relation to the application, the chief officer of the agency concerned shall ensure that no further action is taken by the agency to intercept the communication or to cause it to be intercepted.
- (8) Subsections (4), (5), (6) and (7) only apply where the agency concerned is:

Section 7

- (a) the Australian Federal Police; or
 - (b) the Police Force of a State.
- (9) The doing of an act mentioned in subparagraph (4)(b)(ii) or (iii) or (5)(b)(ii) or (iii) in a particular case is taken to constitute a serious offence, even if it would not constitute a serious offence apart from this subsection.

Note: See subsection (6). A Part 2-5 warrant can only be issued for:

- (a) the purposes of an investigation relating to the commission of one or more serious offences; or
 - (b) purposes relating to a Part 5.3 supervisory order or an application for a post-sentence order.
- (10) Subsection (9) has effect only to the extent necessary:
- (a) to enable an application to be made for the purposes of subsection (6); and
 - (b) to enable a decision to be made on such an application and, if a Judge so decides, a Part 2-5 warrant to be issued; and
 - (c) to enable this Act to operate in relation to a Part 2-5 warrant issued on such an application.

Part 2-2—Warrants authorising the Organisation to intercept telecommunications

9 Issue of telecommunications service warrants by Attorney-General

- (1) Where, upon receipt by the Attorney-General of a request by the Director-General of Security for the issue of a warrant under this section in respect of a telecommunications service, the Attorney-General is satisfied that:
- (a) the telecommunications service is being or is likely to be:
 - (i) used by a person engaged in, or reasonably suspected by the Director-General of Security of being engaged in, or of being likely to engage in, activities prejudicial to security; or
 - (ia) the means by which a person receives or sends a communication from or to another person who is engaged in, or reasonably suspected by the Director-General of Security of being engaged in, or of being likely to engage in, such activities; or
 - (ii) used for purposes prejudicial to security; and
 - (b) the interception by the Organisation of communications made to or from the telecommunications service will, or is likely to, assist the Organisation in carrying out its function of obtaining intelligence relating to security;

the Attorney-General may, by warrant under his or her hand, authorize persons approved under section 12 in respect of the warrant to intercept, subject to any conditions or restrictions that are specified in the warrant, communications that are being made to or from that service and such a warrant may authorize entry on any premises specified in the warrant for the purpose of installing, maintaining, using or recovering any equipment used to intercept such communications.

Note: Subparagraph (a)(ia)—subsection (3) restricts the issuing of warrants if subparagraph (a)(ia) applies.

Section 9A

- (1A) The reference in paragraph (1)(b) to the interception of communications made to or from a telecommunications service includes a reference to the accessing of the communications as stored communications after they have ceased to pass over a telecommunications system.
- (2) A request by the Director-General of Security for the issue of a warrant in respect of a telecommunications service:
- (a) shall include a description of the service sufficient to identify it, including:
 - (i) the name, address and occupation of the subscriber (if any) to the service; and
 - (ii) the number (if any) allotted to the service by a carrier; and
 - (b) shall specify the facts and other grounds on which the Director-General of Security considers it necessary that the warrant should be issued and, where relevant, the grounds on which the Director-General of Security suspects a person of being engaged in, or of being likely to engage in, activities prejudicial to security.
- (3) The Attorney-General must not issue a warrant in a case in which subparagraph (1)(a)(ia) applies unless he or she is satisfied that:
- (a) the Organisation has exhausted all other practicable methods of identifying the telecommunications services used, or likely to be used, by the other person referred to in subparagraph (1)(a)(ia); or
 - (b) interception of communications made to or from a telecommunications service used or likely to be used by that person would not otherwise be possible.

9A Issue of named person warrants by Attorney-General

- (1) Upon receiving a request by the Director-General of Security for the issue of a warrant under this section in respect of a person, the Attorney-General may, under his or her hand, issue a warrant in respect of the person if the Attorney-General is satisfied that:

- (a) the person is engaged in, or reasonably suspected by the Director-General of Security of being engaged in, or of being likely to engage in, activities prejudicial to security; and
 - (b) the interception by the Organisation of:
 - (i) communications made to or from telecommunications services used by the person; or
 - (ii) communications made by means of a particular telecommunications device or particular telecommunications devices used by the person;will, or is likely to, assist the Organisation in carrying out its function of obtaining intelligence relating to security; and
 - (c) relying on a telecommunications service warrant to obtain the intelligence would be ineffective.
- (1A) The warrant authorises persons approved under section 12 in respect of the warrant to intercept, subject to any conditions or restrictions that are specified in the warrant:
- (a) communications that are being made to or from any telecommunications service that the person is using, or is likely to use; or
 - (b) communications that are being made by means of a telecommunications device or telecommunications devices, identified in the warrant, that the person is using, or is likely to use.
- Note: Subsection (3) restricts the issuing of a warrant authorising interception of communications made by means of a telecommunications device or telecommunications devices identified in the warrant.
- (1B) The warrant may authorise entry on any premises specified in the warrant for the purpose of installing, maintaining, using or recovering any equipment used to intercept such communications.
- (1C) The reference in paragraph (1)(b) to the interception of communications made to or from a telecommunications service includes a reference to the accessing of the communications as stored communications after they have ceased to pass over a telecommunications system.

Section 9A

- (2) A request by the Director-General of Security for the issue of a warrant in respect of a person:
- (a) must include the name or names by which the person is known; and
 - (b) must include details (to the extent these are known to the Director-General of Security) sufficient to identify the telecommunications services the person is using, or is likely to use; and
 - (ba) if the warrant would authorise interception of communications made by means of a telecommunications device or telecommunications devices identified in the warrant—must include details (to the extent these are known to the Director-General of Security) sufficient to identify the telecommunications device or telecommunications devices that the person is using, or is likely to use; and
 - (c) must specify the facts and other grounds on which the Director-General of Security considers it necessary that the warrant should be issued, including the grounds on which the Director-General of Security suspects the person of being engaged in, or of being likely to engage in, activities prejudicial to security.
- (3) The Attorney-General must not issue a warrant that authorises interception of communications made by means of a telecommunications device or telecommunications devices identified in the warrant unless he or she is satisfied that:
- (a) there are no other practicable methods available to the Organisation at the time of making the application to identify the telecommunications services used, or likely to be used, by the person in respect of whom the warrant would be issued; or
 - (b) interception of communications made to or from a telecommunications service used, or likely to be used, by that person would not otherwise be practicable.

9B Provisions applying to warrants issued under section 9 or 9A

Request must be forwarded in writing

- (1) Where the Director-General of Security makes a request, otherwise than in writing, for the issue of a warrant under section 9 or 9A, he or she must forthwith forward to the Attorney-General a request in writing for the warrant.

Warrants authorising entry

- (2) Where a warrant under section 9 or 9A authorises entry on premises, the warrant:
 - (a) must state whether entry is authorised to be made at any time of the day or night or only during specified hours; and
 - (b) may, if the Attorney-General thinks fit—provide that entry may be made without permission first being sought or demand first being made, and may authorise measures that he or she is satisfied are necessary for that purpose.

Length of time warrant remains in force

- (3) A warrant under section 9 or 9A must specify the period for which it is to remain in force. The warrant may be revoked by the Attorney-General at any time before the end of the specified period.
- (3A) The specified period must not exceed:
 - (a) if subparagraph 9(1)(a)(ia) applies—3 months; or
 - (b) otherwise—6 months.

Issue of further warrant

- (4) Subsection (3) does not prevent the issue of a further warrant in respect of a telecommunications service or a person (as the case may be) in relation to which or whom a warrant has, or warrants have, previously been issued.

Section 10

10 Issue of warrant by Director-General of Security in emergency for Organisation to intercept telecommunications

(1) Where:

- (a) the Director-General of Security has forwarded or made a request to the Attorney-General for the issue of a warrant under section 9 in respect of a telecommunications service or under section 9A in respect of a person;
- (b) the Attorney-General has not, to the knowledge of the Director-General of Security, made a decision with respect to the request and has not, within the preceding period of 3 months, refused to issue a warrant under section 9 in respect of the telecommunications service or under section 9A in respect of a person (as the case requires);
- (c) the Director-General of Security has not, within the preceding period of 3 months, issued a warrant under this section in respect of the telecommunications service or person (as the case requires); and
- (d) the Director-General of Security is satisfied:
 - (i) that the facts of the case would justify the issue of a warrant by the Attorney-General; and
 - (ii) that, if the interception to which the request relates does not commence before a warrant can be issued and made available by the Attorney-General, security will be, or is likely to be, seriously prejudiced;

the Director-General of Security may, by warrant under his or her hand, authorize persons approved under section 12 in respect of the warrant to intercept, subject to any conditions or restrictions that are specified in the warrant, communications that are being made to or from that service, or communications of that person (as the case requires), and such a warrant may authorize entry on any premises specified in the warrant for the purpose of installing, maintaining, using or recovering any equipment used to intercept such communications.

(1A) The reference in subparagraph (1)(d)(ii) to the interception not commencing includes a reference to the communications, that were

to be intercepted, not being accessed as stored communications after they have ceased to pass over a telecommunications system.

- (2) Where a warrant under this section authorizes entry on premises, the warrant shall state whether entry is authorized to be made at any time of the day or night or only during specified hours and may, if the Director-General of Security thinks fit, provide that entry may be made without permission first being sought or demand first being made, and authorize measures that he or she is satisfied are necessary for that purpose.
- (3) A warrant under this section shall specify the period for which it is to remain in force, being a period that does not exceed 48 hours, but may be revoked by the Attorney-General at any time before the expiration of the period so specified.
- (4) Where the Director-General of Security issues a warrant under this section, he or she shall forthwith furnish to the Attorney-General:
 - (a) a copy of the warrant; and
 - (b) a statement of the grounds on which he or she is satisfied as to the matters referred to in subparagraph (1)(d)(ii).
- (5) The Director-General must, within 3 working days after issuing a warrant under this section, give a copy of the warrant to the Inspector-General of Intelligence and Security.

11A Telecommunications service warrant for collection of foreign intelligence

- (1) Where:
 - (a) the Director-General of Security gives a notice in writing to the Attorney-General requesting the Attorney-General to issue a warrant under this section authorising persons approved under section 12 in respect of the warrant to do acts or things referred to in subsection 9(1) in relation to a particular telecommunications service for the purpose of obtaining foreign intelligence relating to a matter specified in the notice; and

Section 11A

- (b) the Attorney-General is satisfied, on the basis of advice received from the Minister for Defence or the Minister for Foreign Affairs, that the collection of foreign intelligence relating to that matter is in the interests of Australia's national security, Australia's foreign relations or Australia's national economic well-being;
- the Attorney-General may, by warrant under his or her hand, authorise persons approved under section 12 in respect of the warrant, subject to any conditions or restrictions that are specified in the warrant, to do such of those acts or things in relation to that telecommunications service as the Attorney-General considers appropriate in the circumstances and are specified in the warrant, for the purpose of obtaining that intelligence.
- (2) A request by the Director-General of Security for the issue of a warrant under this section:
- (a) shall include a description of the service sufficient to identify it, including:
- (i) the name, address and occupation of the subscriber (if any) to the service; and
- (ii) the number (if any) allotted to the service by a carrier; and
- (b) shall specify the facts and other grounds on which the Director-General of Security considers it necessary that the warrant should be issued.
- (3) If the Director-General of Security requests the issue of a warrant under this section for the purpose of collecting information concerning a person who is an Australian citizen or permanent resident (see subsection 11D(5)), then:
- (a) the Director-General must include details in the request about the grounds on which the Director-General suspects that the person is acting for, or on behalf of, a foreign power; and
- (b) the Attorney-General must not issue the warrant unless the Attorney-General is satisfied that the person is, or is reasonably suspected by the Director-General of, acting for, or on behalf of, a foreign power.

Note: Warrants are obtained under this section for the purpose of performing the function set out in paragraph 17(1)(e) of the *Australian Security Intelligence Organisation Act 1979*.

11B Named person warrant for collection of foreign intelligence

- (1) The Attorney-General may, under his or her hand, issue a warrant in respect of a person if:
- (a) the Director-General of Security gives a notice in writing to the Attorney-General requesting the Attorney-General to issue a warrant under this section authorising persons approved under section 12 in respect of the warrant to do acts or things referred to in subsection 9A(1A) in relation to:
 - (i) communications that are being made to or from any telecommunications service that a person or foreign organisation is using, or is likely to use; or
 - (ii) communications that are being made by means of a particular telecommunications device or particular telecommunications devices that a person or foreign organisation is using, or is likely to use;for the purpose of obtaining foreign intelligence relating to a matter specified in the notice; and
 - (b) the Attorney-General is satisfied, on the basis of advice received from the Minister for Defence or the Minister for Foreign Affairs, that:
 - (i) the obtaining of foreign intelligence relating to that matter is in the interests of Australia's national security, Australia's foreign relations or Australia's national economic well-being; and
 - (ii) it is necessary to intercept the communications of the person or foreign organisation in order to obtain the intelligence referred to in paragraph (a); and
 - (iii) relying on a telecommunications service warrant to obtain the intelligence would be ineffective.
- (1A) The warrant authorises persons approved under section 12 in respect of the warrant to intercept, subject to any conditions or restrictions that are specified in the warrant:

Section 11B

- (a) communications that are being made to or from any telecommunications service that the person or foreign organisation is using, or is likely to use; or
- (b) communications that are being made by means of a telecommunications device or telecommunications devices, identified in the warrant, that the person or foreign organisation is using, or is likely to use.

Note: Subsection (3) restricts the issuing of a warrant authorising interception of communications made by means of a telecommunications device or telecommunications devices identified in the warrant.

- (1B) The warrant may authorise entry on any premises specified in the warrant for the purpose of installing, maintaining, using or recovering any equipment used to intercept such communications.
- (2) A request by the Director-General of Security for the issue of a warrant in respect of a person or foreign organisation:
 - (a) must include the name or names by which the person or organisation is known; and
 - (b) must include details (to the extent these are known to the Director-General of Security) sufficient to identify the telecommunications services the person or foreign organisation is using, or is likely to use; and
 - (ba) if the warrant would authorise interception of communications made by means of a telecommunications device or telecommunications devices identified in the warrant—must include details (to the extent these are known to the Director-General of Security) sufficient to identify the telecommunications device or telecommunications devices that the person is using, or is likely to use; and
 - (c) must specify the facts and other grounds on which the Director-General of Security considers it necessary that the warrant should be issued.
- (3) The Attorney-General must not issue a warrant that authorises interception of communications made by means of a

telecommunications device or telecommunications devices identified in the warrant unless he or she is satisfied that:

- (a) there are no other practicable methods available to the Organisation at the time of making the application to identify the telecommunications services used, or likely to be used, by the person or foreign organisation in respect of whom or which the warrant would be issued; or
 - (b) interception of communications made to or from a telecommunications service used, or likely to be used, by that person or foreign organisation would not otherwise be practicable.
- (4) If the Director-General of Security requests the issue of a warrant under this section for the purpose of collecting information concerning a person who is an Australian citizen or permanent resident (see subsection 11D(5)), then:
- (a) the Director-General must include details in the request about the grounds on which the Director-General suspects that the person is acting for, or on behalf of, a foreign power; and
 - (b) the Attorney-General must not issue the warrant unless the Attorney-General is satisfied that the person is, or is reasonably suspected by the Director-General of, acting for, or on behalf of, a foreign power.

Note: Warrants are obtained under this section for the purpose of performing the function set out in paragraph 17(1)(e) of the *Australian Security Intelligence Organisation Act 1979*.

11C Foreign communications warrant for collection of foreign intelligence

Issue of warrant

- (1) Where:
- (a) the Director-General of Security gives a notice in writing to the Attorney-General requesting the Attorney-General to issue a warrant under this section authorising persons approved under section 12 in respect of the warrant to intercept communications for the purpose of obtaining

Section 11C

foreign intelligence relating to a matter specified in the notice from foreign communications intercepted under the warrant; and

- (b) the Attorney-General is satisfied, on the basis of advice received from the Minister for Defence or the Minister for Foreign Affairs, that:
- (i) the collection of foreign intelligence relating to that matter is in the interests of Australia's national security, Australia's foreign relations or Australia's national economic well-being; and
 - (ii) it is necessary to intercept communications in order to obtain that foreign intelligence from foreign communications intercepted under the warrant; and
 - (iii) relying on a telecommunications service warrant or a named person warrant to obtain the intelligence would be ineffective;

the Attorney-General may, by warrant under his or her hand, authorise persons approved under section 12 in respect of the warrant, subject to any conditions or restrictions that are specified in the warrant, to intercept communications for the purpose of obtaining that foreign intelligence from foreign communications intercepted under the warrant.

- (2) A warrant under subsection (1) must not authorise the interception of any communications except for the purpose of obtaining foreign intelligence relating to a matter specified in the notice referred to in subsection (1) from foreign communications intercepted under the warrant.
- (3) A request by the Director-General of Security for the issue of a warrant under this section must:
- (a) specify how the interception of communications is proposed to be conducted under the warrant, including how the risk of intercepting domestic communications will be minimised; and

- (b) specify the facts and other grounds on which the Director-General of Security considers it necessary that the warrant should be issued, including the reasons the information cannot be collected by other means.
- (3A) If the Director-General of Security requests the issue of a warrant under this section for the purpose of collecting information concerning a person who is an Australian citizen or permanent resident (see subsection 11D(5)), then:
- (a) the Director-General must include details in the request about the grounds on which the Director-General suspects that the person is acting for, or on behalf of, a foreign power; and
 - (b) the Attorney-General must not issue the warrant unless the Attorney-General is satisfied that the person is, or is reasonably suspected by the Director-General of, acting for, or on behalf of, a foreign power.
- (4) The Attorney-General must not issue a warrant under this section if the mandatory procedure under subsection (6) is not in force.
- (4A) If a warrant is issued under this section, then the Director-General of Security must prepare a notice that:
- (a) is addressed to any carrier who operates any part of the telecommunications system that is covered by the warrant; and
 - (b) gives a description that is sufficient to identify that part of the telecommunications system covered by the warrant;
- unless the Attorney-General is satisfied that the giving of such a notice would not be in the interests of national security or reasonable in the circumstances.

Destruction of irrelevant intercepted communications

- (5) Where:
- (a) a communication is intercepted under a warrant under this section; and

Section 11C

- (b) the Director-General of Security is satisfied that the communication is not relevant to the purposes specified in the warrant;

the Director-General of Security must:

- (c) cause all records of the communication to be destroyed (unless the communication relates, or appears to relate, to activities that present a significant risk to a person's life); and
- (d) cause the Inspector-General of Intelligence and Security to be notified of the communication if all records of the communication are not caused to be destroyed because the communication relates, or appears to relate, to activities that present a significant risk to a person's life.

Mandatory procedure for all intercepted communications

- (6) The Attorney-General must, in writing, issue a mandatory procedure (the **mandatory procedure**):
 - (a) for screening communications intercepted under a warrant under this section for the purpose of identifying any domestic communications that may have been intercepted; and
 - (b) for destroying all records of any domestic communication so identified from that screening (other than a domestic communication that relates, or appears to relate, to activities that present a significant risk to a person's life); and
 - (c) for notifying the Inspector-General of Intelligence and Security of any identified domestic communication if all records of the communication are not destroyed because the communication relates, or appears to relate, to activities that present a significant risk to a person's life.
- (7) The mandatory procedure may also deal with other matters relating to communications intercepted under a warrant under this section.
- (8) A person must comply with the mandatory procedure to the extent that it applies to the person.
- (9) Before issuing or varying the mandatory procedure, the Attorney-General must consult:

- (a) the Minister for Defence; and
 - (b) the Minister for Foreign Affairs; and
 - (c) the Inspector-General of Intelligence and Security; and
 - (d) the Director-General of Security.
- (10) The Attorney-General must review the mandatory procedure as soon as practicable after:
- (a) the end of the first anniversary of the mandatory procedure being issued; and
 - (b) every 3-year period after that;
- but the Attorney-General may review the mandatory procedure at any other time as well.
- (10A) The Attorney-General must, as soon as practicable, cause the Parliamentary Joint Committee on Intelligence and Security to be notified about the issuing or varying of the mandatory procedure.
- (10B) The Parliamentary Joint Committee on Intelligence and Security may request a briefing on the mandatory procedure and on any variations to it.
- (11) The mandatory procedure, or any variation of the mandatory procedure, is not a legislative instrument.
- (12) For the purposes of this section, a ***domestic communication*** is a communication that is not a foreign communication.

Note: Warrants are obtained under this section for the purpose of performing the function set out in paragraph 17(1)(e) of the *Australian Security Intelligence Organisation Act 1979*.

11D Provisions applying to foreign intelligence warrants

Warrants authorising entry

- (1) Where a warrant under section 11A or 11B authorises entry on premises, the warrant:
- (a) must state whether entry is authorised to be made at any time of the day or night or only during specified hours; and

Section 11D

- (b) may, if the Attorney-General thinks fit—provide that entry may be made without permission first being sought or demand first being made, and may authorise measures that he or she is satisfied are necessary for that purpose.

Length of time warrant remains in force

- (2) A warrant under section 11A, 11B or 11C must specify the period for which it is to remain in force. The period must not exceed 6 months, and the warrant may be revoked by the Attorney-General at any time before the end of the specified period.

Issue of further warrant

- (3) Subsection (2) does not prevent the issue of a further warrant in respect of a telecommunications service, a person or a part of a telecommunications system (as the case may be) in relation to which or whom a warrant has, or warrants have, previously been issued.

Part 10.6 of the Criminal Code

- (4) Nothing in Part 10.6 of the *Criminal Code* is to be taken to prohibit the doing of anything under, or for the purposes of, a warrant under section 11A, 11B or 11C.

Note: Part 10.6 of the *Criminal Code* deals with offences relating to telecommunications.

Information about Australian citizens or permanent residents

- (5) The Director-General must not request the issue of a warrant under section 11A, 11B or 11C for the purpose of collecting information concerning an Australian citizen or permanent resident, unless the Director-General reasonably suspects that the person is acting for, or on behalf of, a foreign power.
- (6) The reference in subsection 11A(1), 11B(1) and 11C(1) to **conditions or restrictions** includes a reference to conditions or restrictions designed to minimise:

- (a) the obtaining by the Organisation, pursuant to a warrant issued under section 11A, 11B or 11C (as the case may be), of information that is not publicly available concerning Australian citizens or permanent residents; or
- (b) the retention of information of that kind.

12 Persons authorised to intercept communications for Organisation

- (1) The Director-General of Security, or an ASIO employee or ASIO affiliate appointed by the Director-General of Security, in writing, to be an authorizing officer for the purposes of this subsection, may, by writing under his or her hand, approve any persons, or class of persons, as persons authorized to exercise, on behalf of the Organisation, the authority conferred by Part 2-2 warrants.
- (2) To avoid doubt, and without limiting subsection (1), if approval is given to a person or class of persons holding, occupying or performing the duties of an office or position, then the approval extends to such an office or position that comes into existence after the approval is given.
- (3) Subsection (2) does not, by implication, affect the interpretation of any other provision of this Act.
- (4) The Director-General of Security must, as soon as practicable after the authority conferred by a Part 2-2 warrant is exercised on behalf of the Organisation, cause one or more written records to be made that identify each person who exercised that authority.

13 Discontinuance of interception before expiration of warrant

Where, before a Part 2-2 warrant ceases to be in force, the Director-General of Security is satisfied that the grounds on which the warrant was issued have ceased to exist, he or she shall forthwith inform the Attorney-General accordingly and take such steps that are necessary to ensure that the interception of communications under the warrant is discontinued.

Section 14

14 Certain records retained by Organisation to be destroyed

Where:

- (a) a record or copy has been made of a communication intercepted by virtue of a Part 2-2 warrant;
- (b) the record or copy is in the possession or custody, or under the control, of the Organisation; and
- (c) the Director-General of Security is satisfied that the record or copy is not required, and is not likely to be required, in or in connection with the performance by the Organisation of its functions or the exercise of its powers (including the powers conferred by sections 64 and 65);

the Director-General of Security shall cause the record or copy to be destroyed.

Note: See subsection 11C(5) and paragraph 11C(6)(b) for additional rules about the destruction of material obtained under a warrant issued under section 11C.

15 How warrants etc. to be dealt with

(1) Where the Attorney-General issues or revokes a Part 2-2 warrant, he or she shall cause:

- (a) the Director-General of Security to be informed forthwith of the issue of the warrant or of the revocation, as the case may be; and
- (b) the warrant or the instrument of revocation, as the case may be, to be forwarded, as soon as practicable, to the Director General of Security.

(1A) Where:

- (a) the Director-General of Security is informed under paragraph (1)(a) of the issue of a warrant (other than a warrant under section 11C); and
- (b) it is proposed, under the warrant, to intercept communications made to or from a telecommunications service while they are passing over a telecommunications system operated by a carrier; and

(ba) the execution of the warrant will involve the taking of action by the carrier or its employees;

the Director-General of Security shall cause:

(c) an authorised representative of that carrier to be informed forthwith of the issue of the warrant; and

(d) where, under paragraph (1)(b), the Director-General of Security receives the warrant—a copy of the warrant, certified in writing by a certifying person to be a true copy of the warrant, to be given as soon as practicable to that authorised representative.

Note: Subsection 15(7) deals with cases where the Director-General of Security is informed of the issue of a warrant under section 11C.

(1B) Where:

(a) an authorised representative of a carrier has been informed, under subsection (1A), of the issue of a warrant; and

(b) the Director-General of Security is informed under paragraph (1)(a) that the warrant has been revoked;

the Director-General of Security shall cause:

(c) that authorised representative to be informed forthwith of the revocation; and

(d) where, under paragraph (1)(b), the Director-General of Security receives the instrument of revocation—a copy of the instrument, certified in writing by a certifying person to be a true copy of the instrument, to be forwarded as soon as practicable to that authorised representative.

(3) The Attorney-General shall record on each request in writing for the issue of a warrant received by him or her from the Director-General of Security his or her decision with respect to the request and shall cause the request to be returned to the Director-General of Security.

(4) Where:

(a) the Director-General of Security issues a warrant under section 10; and

Section 15

- (b) it is proposed, under the warrant, to intercept communications made to or from a telecommunications service while they are passing over a telecommunications system operated by a carrier; and
 - (ba) the execution of the warrant will involve the taking of action by the carrier or its employees;
- the Director-General of Security shall cause:
- (c) an authorised representative of that carrier to be informed forthwith of the issuing of the warrant; and
 - (d) a copy of the warrant, certified in writing by the Director-General, or a Deputy Director-General of Security, to be a true copy of the warrant, to be given as soon as practicable to that authorised representative.
- (6) The Director-General of Security shall cause to be kept in the Organisation's records:
- (a) each warrant issued under section 10;
 - (c) each warrant, and each instrument of revocation, received under this section by the Director-General from the Attorney-General; and
 - (e) each request, and each document, returned to the Director-General by the Attorney-General.
- (7) Where:
- (a) the Director-General of Security is informed under paragraph (1)(a) of the issue of a warrant under section 11C; and
 - (b) it is proposed, under the warrant, to intercept communications made while they are passing over a telecommunications system operated by a carrier; and
 - (ba) the carrier is required to be given a notice under subsection 11C(4A) in relation to the warrant;
- the Director-General of Security must cause:
- (c) an authorised representative of that carrier to be informed forthwith of the issue of the warrant; and
 - (d) that authorised representative to be given the notice under subsection 11C(4A) as soon as reasonably practicable.
-

16 Additional requirements for named person warrants

(1) Where:

- (a) an authorised representative of a carrier has been given a copy of a warrant under section 9A or 11B; and
- (aa) the warrant is not a warrant that authorises interception of communications made by means of a telecommunications device or telecommunications devices identified in the warrant; and
- (b) it is proposed, under the warrant, to intercept communications made to or from a telecommunications service operated by the carrier; and
- (c) the service was not identified in the warrant;

a certifying person must cause that authorised representative to be given, as soon as practicable, a description in writing of the service sufficient to identify it.

(1A) Where:

- (a) an authorised representative of a carrier has been given a copy of a warrant under section 9A or 11B; and
- (b) the warrant is a warrant that authorises interception of communications made by means of a telecommunications device or telecommunications devices identified in the warrant; and
- (c) it is proposed, under the warrant, to intercept, by means of a telecommunications device, communications made to or from a telecommunications service operated by the carrier; and
- (d) the device was not identified in the warrant;

a certifying person must cause that authorised representative to be given, as soon as practicable, a description in writing of the device sufficient to identify it.

(2) Where:

- (a) an authorised representative of a carrier has been given a description of a telecommunications service to or from which, or a telecommunications device or

Section 17

telecommunications devices by means of which, communications are proposed to be intercepted under a warrant under section 9A or 11B; and

(b) the Director-General of Security is satisfied that the interception of communications to or from that service, or by means of the device or devices, is no longer required;

a certifying person must cause:

(c) that authorised representative to be informed of the fact immediately; and

(d) confirmation in writing of the fact to be given as soon as practicable to that authorised representative.

17 Reports to be made to Attorney-General on results of interception

(1) The Director-General of Security shall furnish to the Attorney-General, in respect of each Part 2-2 warrant, within 3 months after the expiration or revocation, whichever first occurs, of the warrant, a report in writing on the extent to which the interception of communications under the warrant has assisted the Organisation in carrying out its functions.

(2) A report under subsection (1) in relation to a warrant issued under section 9A or 11B must include details of the telecommunications service to or from which each intercepted communication was made.

18 Evidentiary certificates

(1) The following:

(a) the Managing Director of a carrier;

(b) the secretary of a carrier;

(c) an employee of a carrier authorised in writing for the purposes of this paragraph by the Managing Director or the secretary of the carrier;

may issue a written certificate signed by him or her setting out such facts as he or she considers relevant with respect to acts or things

done by, or in relation to, employees of the carrier in order to enable a warrant to be executed.

- (2) A document purporting to be a certificate issued under subsection (1) and purporting to be signed by the Managing Director or secretary, or an employee, of a carrier is to be received in evidence in an exempt proceeding without further proof and is, in an exempt proceeding, conclusive evidence of the matters stated in the document.
- (3) The Director-General of Security or the Deputy Director-General of Security may issue a written certificate signed by him or her setting out such facts as he or she considers relevant with respect to acts or things done:
 - (a) in order to enable, or in connection with enabling, a warrant issued under this Part to be executed; or
 - (b) in connection with the execution of a warrant issued under this Part.
- (4) The Director-General of Security or the Deputy Director-General of Security may issue a written certificate signed by him or her setting out such facts as he or she considers relevant with respect to anything done by an ASIO employee or an ASIO affiliate:
 - (a) in connection with the execution of a warrant issued under this Part; or
 - (b) in connection with:
 - (i) the communication by a person to another person of; or
 - (ii) the making use of; or
 - (iii) the making of a record of; or
 - (iv) the custody of a record of; or
 - (v) the giving in evidence of;information obtained by the execution of such a warrant.
- (5) A document purporting to be a certificate issued under subsection (3) or (4) by the Director-General of Security or the Deputy Director-General of Security and to be signed by him or her is to be received in evidence in an exempt proceeding without

Section 18

further proof and is, in an exempt proceeding, prima facie evidence of the matters stated in the document.

- (6) In subsections (1) and (2), a reference to the Managing Director or secretary of a carrier includes a reference to the Managing Director or secretary of a body corporate of which the carrier is a subsidiary.
- (7) For the purposes of this section, the question whether a body corporate is a subsidiary of another body corporate is to be determined in the same manner as the question is determined under the *Corporations Act 2001*.

Part 2-3—Emergency requests authorising officers of a carrier to intercept telecommunications

30 Emergency requests

(1) Where:

- (a) a person is a party to a communication passing over a telecommunications system;
- (b) as a result of information conveyed by another party to the communication (in this section referred to as the *caller*) and of any other matters, the first-mentioned person forms the honest belief that either of the following emergencies exist:
 - (i) another person (whether or not the caller) is dying, is being seriously injured or has been seriously injured;
 - (ii) another person (whether or not the caller) is likely to die or be seriously injured; and
- (c) the first-mentioned person does not know the location of the caller;

the first-mentioned person may:

- (d) in a case where the first-mentioned person:
 - (i) is a member of a police force; and
 - (ii) is of the opinion that tracing the location of the caller is likely to be of assistance in dealing with the emergency;request, or cause another member of a police force to request, an employee of a carrier to intercept, or to cause other employees of the carrier to intercept, the communication for the purposes of tracing the location of the caller; or
- (e) in a case where the first-mentioned person is not a member of a police force—inform, or cause another person to inform, a member of a police force of the matters referred to in paragraphs (a), (b) and (c).

Section 30

- (2) Where a member of a police force is so informed, the member may, if the member is of the opinion that tracing the location of the caller is likely to be of assistance in dealing with the emergency, request an employee of a carrier to intercept, or to cause other employees of the carrier to intercept, the communication for the purposes of tracing the location of the caller.
- (3) Where, pursuant to a request made, or purporting to be made, by a member of a police force under subsection (1) or (2), an employee of a carrier intercepts a communication passing over a telecommunications system for the purpose of tracing the location of the caller, the employee shall:
 - (a) communicate, or cause another employee of the carrier to communicate, the location of the caller to the person who made the request or to any other member of a police force; and
 - (b) communicate particulars of the interception to the Managing Director of the carrier.
- (4) As soon as practicable after making to an employee of a carrier a request under, or purporting to be under, subsection (1) or (2), a member of a police force shall give, or cause another member of a police force to give, to the Managing Director of the carrier a written confirmation of the request that sets out the information given by the first-mentioned member to that employee in connection with the request.

Part 2-4—Authorisation of interception for developing and testing interception capabilities

31 Applications for authorisation

- (1) The head (however described) of a security authority that has functions that include activities relating to developing or testing technologies, or interception capabilities, or a person acting as that head, may request the Attorney-General to authorise, under section 31A, interception of communications passing over a telecommunications system:
 - (a) if one or more carriers are specified in the request for the purposes of this paragraph—by:
 - (i) employees of the security authority authorised under section 31B; and
 - (ii) employees of those carriers; or
 - (b) if no carriers are specified in the request for the purposes of paragraph (a)—by employees of the security authority authorised under section 31B.
- (2) The request:
 - (a) must be in writing; and
 - (b) must include details of the development or testing of technologies, or interception capabilities, in relation to which authorisation is sought; and
 - (c) must include details of the extent to which the development or testing would involve, or would be likely to involve, interception of communications passing over a telecommunications system; and
 - (d) must refer to the functions of the authority that the development or testing would support; and
 - (e) must state the grounds for seeking the authorisation; and

Section 31A

- (f) must summarise the outcomes of any previous authorisations given to the authority under section 31A in relation to the technology or interception capability that is the subject of the application; and
- (g) must nominate the period (not exceeding 6 months) for which the authorisation is sought to be in force.

31A Attorney-General may authorise interception for developing and testing interception capabilities

- (1) Upon receiving the request, the Attorney-General may authorise interception of communications passing over a telecommunications system:
 - (a) if one or more carriers are specified in the request for the purposes of paragraph 31(1)(a)—by:
 - (i) employees of the security authority authorised under section 31B; and
 - (ii) employees of those carriers; or
 - (b) if no carriers are specified in the request for the purposes of paragraph 31(1)(a)—by employees of the security authority authorised under section 31B.
- (2) The authorisation is subject to:
 - (a) a condition prohibiting:
 - (i) interception of communications passing over a telecommunications system except for the purposes of development or testing of technologies, or interception capabilities; or
 - (ii) communicating, using or recording such communications except for such purposes; and
 - (b) any other conditions specified in the authorisation.
- (3) The authorisation must be in writing and must specify the period (not exceeding 6 months) for which it will have effect.
- (4) The head (however described) of the security authority, or a person acting as that head, must ensure that a copy of the authorisation is

Section 31AA

kept by the authority and is available for inspection on request by the Minister who is responsible for the authority.

- (4A) If paragraph (1)(a) applies to the authorisation, this Part does not require that an authorised interception must involve:
- (a) one or more employees of the security authority referred to in that paragraph; and
 - (b) one or more employees of a carrier referred to in that paragraph;
- acting together or in the presence of each other.
- (5) An authorisation given under subsection (1) is not a legislative instrument.

31AA Carrier to be notified of authorisation etc.

- (1) If:
- (a) the Attorney-General gives a section 31A authorisation in response to an application made by:
 - (i) the head (however described) of a security authority; or
 - (ii) a person acting as that head; and
 - (b) the authorisation covers the employees of a carrier;
- the head (however described) of the security authority, or a person acting as that head, must cause a copy of the authorisation to be given to the authorised representative of the carrier as soon as practicable.
- (2) If:
- (a) the Attorney-General has given a section 31A authorisation in response to an application made by:
 - (i) the head (however described) of a security authority; or
 - (ii) a person acting as that head; and
 - (b) the authorisation is varied or revoked; and
 - (c) the authorisation covers the employees of a carrier;
- the head (however described) of the security authority, or a person acting as that head, must cause:

Section 31B

- (d) an authorised representative of the carrier to be immediately informed of the variation or revocation; and
- (e) a copy of the variation or revocation to be given to the authorised representative as soon as practicable.

31B Authorisation of employees of a security authority

- (1) The following persons:
 - (a) the head (however described) of a security authority;
 - (b) an officer of the security authority covered by an approval in force under subsection (2);may, by writing, authorise employees of the authority for the purposes of this Part.
- (2) The head (however described) of a security authority may, by writing, approve an officer of the authority for the purposes of paragraph (1)(b).

31C Destruction of records

If:

- (a) information, or a record, that was obtained, in the course of developing or testing technologies or interception capabilities, by interception of communications passing over a telecommunications system is in a security authority's possession; and
 - (b) the information or record is no longer required in relation to the development or testing;
- the head (however described) of the security authority, or a person acting as that head, must cause the information or record to be destroyed as soon as practicable.

31D Reports to the Attorney-General

The head (however described) of a security authority, or a person acting as that head, must give to the Attorney-General, within 3

Section 31E

months after an authorisation under section 31A given to the authority ceases to have effect, a written report about:

- (a) the outcome of the development or testing of technologies, or interception capabilities, in relation to which the authorisation was given; and
- (b) the destruction of information or records under section 31C.

31E Employees of security authorities

- (1) For the purposes of this Part:
 - (a) an ASIO employee is taken to be an employee of the Organisation; and
 - (b) an ASIO affiliate is taken to be an employee of the Organisation.
- (2) For the purposes of this Part, if:
 - (a) a person is a staff member (within the meaning of the *Intelligence Services Act 2001*) of an agency (within the meaning of that Act); and
 - (b) the agency is a security authority;the person is taken to be an employee of the security authority.

Part 2-5—Warrants authorising agencies to intercept telecommunications

Division 2—Declaration of State Law Enforcement Authorities as Agencies

34 Declaration of an eligible authority of a State as an agency

Subject to section 35, the Minister may, by legislative instrument and at the request of the Premier of a State, declare an eligible authority of that State to be an agency for the purposes of this Act.

Note: The declaration may also authorise the eligible authority to apply for Part 5.3 warrants: see section 38A.

35 Preconditions for declaration

- (1) The Minister shall not make a declaration under section 34 in relation to an eligible authority of a State unless he or she is satisfied that the law (in this subsection called the *relevant law*) of that State makes satisfactory provision:
 - (a) imposing on the chief officer of the eligible authority requirements corresponding to the requirements that section 80 (other than paragraphs 80(f) and (g)) and section 81 (other than paragraph 81(1)(h), and subsection 81(2), so far as that subsection relates to paragraph 81(1)(h)) impose on the chief officer of a Commonwealth agency; and
 - (c) requiring the chief officer of the eligible authority to give to a specified Minister (in this subsection called the *responsible Minister*) of that State, within 3 months after a warrant issued to the eligible authority ceases to be in force, a written report about:
 - (i) the use made by the eligible authority of information obtained by interceptions under the warrant; and

- (ii) the communication of such information to persons other than officers of the eligible authority; and
- (d) requiring the chief officer of the eligible authority to give to the responsible Minister as soon as practicable, and in any event within 3 months, after each 30 June, a written report that sets out such information as:
 - (i) Division 2 of Part 2-8 requires to be set out in the Minister's report under that Division relating to the year ending on that 30 June; and
 - (ii) can be derived from the eligible authority's records; and
- (e) requiring the responsible Minister to give to the Minister, as soon as practicable after a report of a kind referred to in paragraph (c) or (d) is given to the responsible Minister, a copy of the report; and
- (f) requiring the chief officer of the eligible authority to cause a restricted record (whether made before or after the commencement of this section) that is in the possession of the eligible authority to be kept, except when it is being otherwise dealt with in accordance with this Act and the relevant law, in a secure place where it is not accessible to persons other than persons who are entitled so to deal with it; and
- (g) requiring the chief officer of the eligible authority to cause a restricted record of a kind referred to in paragraph (f) to be destroyed forthwith where the chief officer is satisfied that the restricted record is not likely to be required for a permitted purpose in relation to the eligible authority, other than a purpose connected with an inspection of the kind referred to in paragraph (h) or with a report on such an inspection; and
- (h) requiring regular inspections of the eligible authority's records, for the purpose of ascertaining the extent of compliance by the officers of the eligible authority with the requirements referred to in paragraphs (a), (f) and (g) of this subsection, to be made by an authority of that State that is independent of the eligible authority and on which sufficient powers have been conferred to enable the independent

Section 35

authority to make a proper inspection of those records for that purpose; and

- (ha) requiring that a person who performs a function or exercises a power under section 44A or 45 in relation to an application by an eligible authority for a warrant must not undertake an inspection of the eligible authority's records for the purpose referred to in paragraph (h) in relation to a record of the eligible authority that relates to the application; and
 - (j) requiring an authority of that State that has made an inspection of the eligible authority's interception records for the purpose referred to in paragraph (h) to report in writing to the responsible Minister about the results of the inspection; and
 - (k) empowering an authority of that State that, as a result of inspecting the eligible authority's records for the purpose referred to in paragraph (h), is of the opinion that an officer of the eligible authority has contravened:
 - (i) a provision of this Act; or
 - (ii) a requirement referred to in paragraph (c);to include in the report on the inspection a report on the contravention; and
 - (m) requiring the responsible Minister to give to the Minister, as soon as practicable after a report on an inspection of the kind referred to in paragraph (j) is given to the responsible Minister, a copy of the report.
- (1A) Paragraphs (1)(f) and (g) do not apply to a restricted record that is a record of a communication that was intercepted under paragraph 7(2)(aaa).
- (2) The Minister must not make a declaration under section 34 in relation to an eligible authority of a State unless the Minister is satisfied that that State has entered into an agreement to pay all expenses connected with the issue of warrants to the authority.

36 State laws requiring copies of documents to be given to responsible Minister

- (1) Nothing in this Division is to be taken to preclude a law of a State from requiring the chief officer of the eligible authority to give to a specified Minister (the *responsible Minister*) of that State a copy of each warrant issued to the eligible authority, and of each instrument under section 52 or 57 revoking such a warrant.
- (2) If a State makes a law of the kind mentioned in subsection (1), then, for the purposes of section 63AA, the chief officer of the eligible authority is taken to be communicating interception warrant information for the purposes of this Part by giving documents to the responsible Minister to comply with the requirement.

37 Revocation of declaration

- (1) If requested by the Premier of a State to revoke a declaration in force under section 34 in relation to an eligible authority of that State, the Minister shall, by notice in writing published in the *Gazette*, revoke the declaration.
- (2) Subject to subsection (1), the Minister may, by notice in writing published in the *Gazette*, revoke a declaration in force under section 34 in relation to an eligible authority of a State if, and only if, the Minister is satisfied that:
 - (a) the law of that State no longer makes satisfactory provision in relation to the authority as mentioned in subsection 35(1);
 - (b) the extent of compliance with a requirement of a law of that State, being a requirement of a kind referred to in subsection 35(1), has been unsatisfactory in so far as the requirement relates to the authority;
 - (c) no agreement of the kind referred to in subsection 35(2), being an agreement entered into by that State that relates to the authority, is in force;
 - (d) the extent of compliance by that State with the terms of an agreement of the kind referred to in subsection 35(2), being

Section 38

an agreement entered into by that State, has been unsatisfactory in so far as the agreement relates to the authority; or

- (e) the extent of compliance by the chief officer of the authority, or by officers of the authority, with this Act has been unsatisfactory.

38 Effect of revocation

Where a declaration under section 34 in relation to an eligible authority of a State is revoked, this Act:

- (a) continues to apply in relation to a warrant that was issued to the authority before the revocation; and
(b) so applies at a particular time as if the authority were an agency at that time.

38A Agencies authorised to apply for Part 5.3 warrants

- (1) This section applies to a declaration made under section 34 in relation to an eligible authority of a State.

Authorisation

- (2) When the Minister makes the declaration, the Minister must, in the declaration, authorise the eligible authority to apply for Part 5.3 warrants if:
- (a) the Premier of the State requests that the eligible authority be so authorised; and
(b) the Minister is satisfied as mentioned in subsection (4) of this section.
- (3) The Minister must amend the declaration to authorise the eligible authority to apply for Part 5.3 warrants if:
- (a) the declaration does not already so authorise the eligible authority; and
(b) the Premier of the State requests that the eligible authority be so authorised; and
(c) the Minister is satisfied as mentioned in subsection (4).

Criteria to be authorised to apply for a Part 5.3 warrant

- (4) For the purposes of paragraph (2)(b) or (3)(c), the Minister must be satisfied that the law of the State makes satisfactory provision:
- (a) imposing on the chief officer of the eligible authority requirements corresponding to the requirements that paragraphs 80(f) and (g) and 81(1)(h) and subsection 81(2), so far as that subsection relates to paragraph 81(1)(h), impose on the chief officer of a Commonwealth agency; and
 - (b) imposing on the chief officer of the eligible authority requirements corresponding to the requirements that section 59B imposes on the chief officer of a Commonwealth agency; and
 - (c) giving an authority of the State powers corresponding to those that subsections 83(3) and 84(2) and sections 85 and 85A give to the Ombudsman, if the authority of the State receives a notice from the eligible authority because of the requirements mentioned in paragraph (b) of this subsection; and
 - (d) requiring an authority of the State that has made an inspection of the eligible authority's records under the powers mentioned in paragraph (c) to report in writing to the responsible Minister about the results of the inspection; and
 - (e) requiring the responsible Minister to give to the Minister, as soon as practicable, a copy of a report that an authority of the State gives to the responsible Minister under a power or requirement mentioned in paragraph (c) or (d).

Removal of authorisation

- (5) The Minister must amend the declaration to remove the authorisation of the eligible authority to apply for Part 5.3 warrants if the Premier of the State requests the Minister to remove the authorisation.
- (6) The Minister may amend the declaration to remove the authorisation of the eligible authority to apply for Part 5.3 warrants if the Minister is satisfied that:

Chapter 2 Interception of telecommunications

Part 2-5 Warrants authorising agencies to intercept telecommunications

Division 2 Declaration of State Law Enforcement Authorities as Agencies

Section 38A

- (a) the law of the State no longer makes satisfactory provision in relation to the eligible authority as mentioned in subsection (4); or
 - (b) the extent of compliance with a requirement of a law of that State, being a requirement of a kind mentioned in subsection (4), has been unsatisfactory in so far as the requirement relates to the eligible authority; or
 - (c) the extent of compliance by the chief officer of the eligible authority, or by officers of the eligible authority, with this Act has been unsatisfactory, so far as this Act relates to Part 5.3 warrants.
- (7) If the Minister amends the declaration under subsection (5) or (6), the amendment does not affect the validity of a Part 5.3 warrant issued before the amendment in response to an application by the eligible authority.

Division 3—Applications for warrants

39 Agency may apply for warrant

- (1) An agency may apply to an eligible Judge or nominated AAT member for a warrant in respect of a telecommunications service or a person.
- (2) An application for a warrant shall be made on an agency's behalf by:
 - (a) in the case of the Australian Federal Police—a member of the Australian Federal Police; or
 - (aa) in the case of the Australian Commission for Law Enforcement Integrity:
 - (i) the Integrity Commissioner; or
 - (ii) an Assistant Integrity Commissioner; or
 - (iii) a staff member of ACLEI who is authorised in writing by the Integrity Commissioner for the purposes of this paragraph; or
 - (b) in the case of the ACC:
 - (i) the Chief Executive Officer of the ACC or an examiner; or
 - (ii) a member of a police force who is a member of the staff of the ACC; or
 - (c) in the case of the Police Force of a State—an officer of that Police Force; or
 - (d) in the case of the Crime Commission:
 - (i) a member of the Crime Commission; or
 - (ii) a member of the staff of the Crime Commission; or
 - (e) in the case of the Independent Commission Against Corruption—an officer of that Commission; or
 - (ea) in the case of the IBAC—an IBAC officer; or
 - (f) in the case of the Crime and Corruption Commission—a commission officer (within the meaning of the Crime and Corruption Act); or

Section 40

- (g) in the case of the Law Enforcement Conduct Commission:
 - (i) the Chief Commissioner of the Commission; or
 - (ii) the Commissioner for Integrity of the Commission; or
 - (iii) an Assistant Commissioner of the Commission; or
 - (iv) a member of the staff of the Law Enforcement Conduct Commission; or
- (i) in the case of the Corruption and Crime Commission—an officer of the Corruption and Crime Commission; or
- (j) in the case of the Independent Commissioner Against Corruption:
 - (i) the Independent Commissioner Against Corruption; or
 - (ii) the Deputy Commissioner referred to in section 9 of the Independent Commissioner Against Corruption Act; or
 - (iii) a member of the staff of the Independent Commissioner Against Corruption.

40 Form of application

- (1) Subject to subsection (2), an application for a warrant shall be in writing.
- (2) If the person making an application for a warrant on an agency's behalf:
 - (a) is the chief officer of the agency or a person in relation to whom an authorisation by the chief officer is in force under subsection (3); and
 - (b) thinks it necessary, because of urgent circumstances, to make the application by telephone;the person may make the application by telephone.
- (3) The chief officer of an agency may authorise in writing, for the purposes of subsection (2), persons who, or classes of persons who, are entitled under section 39 to make applications on the agency's behalf.

41 Contents of application

A written application by an agency for a warrant shall set out:

- (a) the name of the agency; and
- (b) the name of the person making the application on the agency's behalf.

42 Affidavit to accompany written application

- (1) A written application by an agency for a warrant shall be accompanied by an affidavit complying with this section.
- (2) The affidavit shall set out the facts and other grounds on which the application is based.
- (3) The affidavit shall specify the period for which it is requested that the warrant be in force and shall state why it is considered necessary for the warrant to be in force for that period.
- (4) If the application is for a telecommunications service warrant, the affidavit shall set out, in relation to the service, and in relation to each person to whom the application relates, the following information, so far as it can be derived from the agency's records:
 - (a) the number of previous applications (if any) for warrants that the agency has made and that related to the service or to that person, as the case may be;
 - (b) the number of warrants (if any) previously issued on such applications; and
 - (c) particulars of the use made by the agency of information obtained by interceptions under such warrants.
- (4A) If the application is for a named person warrant, the affidavit must set out:
 - (a) the name or names by which the person is known; and
 - (b) details (to the extent these are known to the chief officer) sufficient to identify the telecommunications services the person is using, or is likely to use; and

Section 43

- (ba) if the warrant would authorise interception of communications made by means of a telecommunications device or telecommunications devices identified in the warrant—details (to the extent these are known to the chief officer) sufficient to identify the telecommunications device or telecommunications devices that the person is using, or is likely to use; and
 - (c) the number of previous applications (if any) for warrants that the agency has made and that related to the person or to a service that the person has used; and
 - (d) the number of warrants (if any) previously issued on such applications; and
 - (e) particulars of the use made by the agency of information obtained by interceptions under such warrants.
- (5) Notwithstanding subsection (1), a written application may be accompanied by 2 or more affidavits that together set out each matter that, but for this subsection, this section would have required an affidavit accompanying the application to set out, specify or state.

43 Information to be given on telephone application

The information given to a Judge or nominated AAT member in connection with a telephone application to the Judge or nominated AAT member:

- (a) shall include particulars of the urgent circumstances because of which the person making the application on the agency's behalf thinks it necessary to make the application by telephone;
- (b) shall include each matter that, if the application had been made in writing, section 41, 42 or 48 would have required the application, or an affidavit accompanying it, to set out, specify or state; and
- (c) shall be given orally or in writing, as the Judge or nominated AAT member directs.

44 Giving further information to Judge

- (1) A Judge or nominated AAT member may require further information to be given in connection with an application to the Judge or nominated AAT member for a warrant.
- (2) The further information:
 - (a) shall be given on oath if the application was made in writing; and
 - (b) shall be given orally or otherwise, as the Judge or nominated AAT member directs.

44A Application by interception agency of Victoria

Scope

- (1) This section applies if an interception agency of Victoria applies, under section 39, to an eligible Judge or nominated AAT member for a warrant in respect of a telecommunications service or a person.

PIM may make submissions

- (2) A Victorian PIM may, orally or in writing, make submissions to the Judge or nominated AAT member about the following matters:
 - (a) in relation to an application for a warrant in respect of a telecommunications service—the matters mentioned in paragraphs 46(2)(a) to (f), 46(5)(a) to (f) or 46(8)(a) to (e), as the case requires;
 - (b) in relation to an application for a warrant in respect of a person—the matters mentioned in paragraphs 46A(2)(a) to (f), 46A(2B)(a) to (f) or 46A(2D)(a) to (e), as the case requires.

PIM may question certain persons

- (3) The Victorian PIM may, for the purpose of making submissions under subsection (2), question:

Section 45

- (a) the person making the application for the warrant on the interception agency's behalf; or
- (b) a person who, under section 44, is required by the Judge or nominated AAT member to give further information to the Judge or nominated AAT member in connection with the application.

However, the Victorian PIM may only do so in the presence of the eligible Judge or nominated AAT member.

45 Application by interception agency of Queensland

Scope

- (1) This section applies if an interception agency of Queensland applies, under section 39, to an eligible Judge or nominated AAT member for a warrant in respect of a telecommunications service or a person.

PIM may make submissions

- (2) A Queensland PIM may, orally or in writing, make submissions to the Judge or nominated AAT member about the following matters:
 - (a) in relation to an application for a warrant in respect of a telecommunications service—the matters mentioned in paragraphs 46(2)(a) to (f), 46(5)(a) to (f) or 46(8)(a) to (e), as the case requires;
 - (b) in relation to an application for a warrant in respect of a person—the matters mentioned in paragraphs 46A(2)(a) to (f), 46A(2B)(a) to (f) or 46A(2D)(a) to (e), as the case requires.

PIM may question certain persons

- (3) The Queensland PIM may, for the purpose of making submissions under subsection (2), question:
 - (a) the person making the application for the warrant on the interception agency's behalf; or

(b) a person who, under section 44, is required by the Judge or nominated AAT member to give further information to the Judge or nominated AAT member in connection with the application.

However, the Queensland PIM may only do so in the presence of the eligible Judge or nominated AAT member.

- (4) A Queensland PIM may delegate to a Queensland deputy PIM the Queensland PIM's power under subsection (2) or (3), or both. The delegation must be in writing.
- (5) In exercising powers under the delegation, the Queensland deputy PIM must comply with any directions of the Queensland PIM.

45A State law not affected

If:

- (a) a person (the **applicant**) applies, or proposes to apply, under section 39, on behalf of an interception agency of Victoria or Queensland for a warrant in respect of a telecommunications service or a person; and
- (b) a law of that State authorises or requires the applicant:
- (i) to notify the PIM of that State of the application or proposed application; or
 - (ii) to notify the PIM of that State of any information that relates to the application or proposed application; or
 - (iii) to give the PIM of that State any document that relates to the application or proposed application;

then nothing in this Act prevents the applicant from making the notification or giving the document to the PIM of that State.

Division 4—Warrants

46 Issue of telecommunications service warrant

Warrant relating to the investigation of one or more serious offences

- (1) Where an agency applies to an eligible Judge or nominated AAT member for a warrant in respect of a telecommunications service and the Judge or nominated AAT member is satisfied, on the basis of the information given to the Judge or nominated AAT member under this Part in connection with the application, that:
- (a) Division 3 has been complied with in relation to the application; and
 - (b) in the case of a telephone application—because of urgent circumstances, it was necessary to make the application by telephone; and
 - (c) there are reasonable grounds for suspecting that a particular person is using, or is likely to use, the service; and
 - (d) information that would be likely to be obtained by intercepting under a warrant communications made to or from the service would be likely to assist in connection with the investigation by the agency of a serious offence, or serious offences, in which:
 - (i) the particular person is involved; or
 - (ii) another person is involved with whom the particular person is likely to communicate using the service; and
 - (e) having regard to the matters referred to in subsection (2), and to no other matters, the Judge or nominated AAT member should issue a warrant authorising such communications to be intercepted;

the Judge or nominated AAT member may, in his or her discretion, issue such a warrant.

Note: Subparagraph (d)(ii)—subsection (3) restricts the issuing of warrants if subparagraph (d)(ii) applies.

- (2) For the purposes of subsection (1), the matters to which the Judge or nominated AAT member shall have regard are:
- (a) how much the privacy of any person or persons would be likely to be interfered with by intercepting under a warrant communications made to or from the service referred to in subsection (1); and
 - (b) the gravity of the conduct constituting the offence or offences being investigated; and
 - (c) how much the information referred to in paragraph (1)(d) would be likely to assist in connection with the investigation by the agency of the offence or offences; and
 - (d) to what extent methods of investigating the offence or offences that do not involve so intercepting communications have been used by, or are available to, the agency; and
 - (e) how much the use of such methods would be likely to assist in connection with the investigation by the agency of the offence or offences; and
 - (f) how much the use of such methods would be likely to prejudice the investigation by the agency of the offence or offences, whether because of delay or for any other reason; and
 - (fa) in relation to an application by an interception agency of Victoria—any submissions made by the Victorian PIM under section 44A to the Judge or nominated AAT member; and
 - (g) in relation to an application by an interception agency of Queensland—any submissions made by the Queensland PIM under section 45 to the Judge or nominated AAT member.
- (3) The Judge or nominated AAT member must not issue a warrant under subsection (1) in a case in which subparagraph (1)(d)(ii) applies unless he or she is satisfied that:
- (a) the agency has exhausted all other practicable methods of identifying the telecommunications services used, or likely to be used, by the person involved in the offence or offences referred to in paragraph (1)(d); or

Section 46

- (b) interception of communications made to or from a telecommunications service used or likely to be used by that person would not otherwise be possible.

Warrant sought for Part 5.3 supervisory order

- (4) If a Part 5.3 warrant agency applies to an eligible Judge or nominated AAT member for a warrant in respect of a telecommunications service and the Judge or nominated AAT member is satisfied, on the basis of the information given to the Judge or nominated AAT member under this Part in connection with the application, that:
 - (a) Division 3 has been complied with in relation to the application; and
 - (b) in the case of a telephone application—because of urgent circumstances, it was necessary to make the application by telephone; and
 - (c) there are reasonable grounds for suspecting that a particular person is using, or is likely to use, the service; and
 - (d) either:
 - (i) a Part 5.3 supervisory order is in force in relation to the particular person; or
 - (ii) a Part 5.3 supervisory order is in force in relation to another person, and the particular person is likely to communicate with the other person using the service; and
 - (e) information that would be likely to be obtained by intercepting under a warrant communications made to or from the service would be likely to substantially assist in connection with:
 - (i) achieving a Part 5.3 object; or
 - (ii) determining whether the Part 5.3 supervisory order, or any succeeding Part 5.3 supervisory order, has been, or is being, complied with; and
 - (f) having regard to the matters referred to in subsection (5), and to no other matters, the Judge or nominated AAT member

should issue a warrant authorising such communications to be intercepted;

the Judge or nominated AAT member may, in his or her discretion, issue such a warrant.

Note 1: Subsection (6) restricts the issuing of warrants if subparagraph (d)(ii) applies.

Note 2: For Part 5.3 supervisory orders that have been made but not come into force, see section 6T.

- (5) For the purposes of subsection (4), the matters to which the Judge or nominated AAT member must have regard are:
- (a) how much the privacy of any person or persons would be likely to be interfered with by intercepting under a warrant communications made to or from the service referred to in subsection (4); and
 - (b) how much the information referred to in paragraph (4)(e) would be likely to assist in connection with:
 - (i) achieving a Part 5.3 object; or
 - (ii) determining whether the Part 5.3 supervisory order, or any succeeding Part 5.3 supervisory order, has been, or is being, complied with; and
 - (c) to what extent methods for:
 - (i) achieving a Part 5.3 object; or
 - (ii) determining whether the Part 5.3 supervisory order, or any succeeding Part 5.3 supervisory order, has been, or is being, complied with;that do not involve so intercepting communications have been used by, or are available to, the agency; and
 - (d) how much the use of such methods would be likely to assist in connection with:
 - (i) achieving a Part 5.3 object; or
 - (ii) determining whether the Part 5.3 supervisory order, or any succeeding Part 5.3 supervisory order, has been, or is being, complied with; and
 - (e) how much the use of such methods would be likely to prejudice:

Section 46

- (i) achieving a Part 5.3 object; or
- (ii) determining whether the Part 5.3 supervisory order, or any succeeding Part 5.3 supervisory order, has been, or is being, complied with;
whether because of delay or for any other reason; and
- (f) whether intercepting under a warrant communications made to or from the service referred to in subsection (4) would be the method that is likely to have the least interference with any person's privacy; and
- (g) in relation to a Part 5.3 supervisory order that is a control order—the possibility that the person in relation to whom the control order is in force:
 - (i) has engaged, is engaging, or will engage, in a terrorist act; or
 - (ii) has provided, is providing, or will provide, support for a terrorist act; or
 - (iii) has facilitated, is facilitating, or will facilitate, a terrorist act; or
 - (iv) has provided, is providing, or will provide, support for the engagement in a hostile activity in a foreign country; or
 - (v) has facilitated, is facilitating, or will facilitate, the engagement in a hostile activity in a foreign country; and
- (ga) in relation to a Part 5.3 supervisory order that is an extended supervision order or interim supervision order—the possibility that the person in relation to whom the order is in force has committed, is committing, or will commit a serious Part 5.3 offence; and
- (gb) in relation to any Part 5.3 supervisory order—the possibility that the person in relation to whom the order is in force:
 - (i) has contravened, is contravening or will contravene the Part 5.3 supervisory order; or
 - (ii) will contravene a succeeding Part 5.3 supervisory order; and

- (h) in relation to an application by an interception agency of Victoria—any submissions made by the Victorian PIM under section 44A to the Judge or nominated AAT member; and
 - (i) in relation to an application by an interception agency of Queensland—any submissions made by the Queensland PIM under section 45 to the Judge or nominated AAT member.
- (6) The Judge or nominated AAT member must not issue a warrant in a case in which subparagraph (4)(d)(ii) applies unless he or she is satisfied that:
- (a) the agency has exhausted all other practicable methods of identifying the telecommunications services used, or likely to be used, by the person to whom the Part 5.3 supervisory order referred to in subparagraph (4)(d)(ii) relates; or
 - (b) interception of communications made to or from a telecommunications service used or likely to be used by that person would not otherwise be possible.

Warrant sought for post-sentence order application

- (7) If a Part 5.3 warrant agency applies to an eligible Judge or nominated AAT member for a warrant in respect of a telecommunications service and the Judge or nominated AAT member is satisfied, on the basis of the information given to the Judge or nominated AAT member under this Part in connection with the application, that:
- (a) Division 3 has been complied with in relation to the application; and
 - (b) in the case of a telephone application—because of urgent circumstances, it was necessary to make the application by telephone; and
 - (c) there are reasonable grounds for suspecting that a particular person is using, or is likely to use, the service; and
 - (d) the person is a terrorist offender in relation to whom an application for a post-sentence order could be made; and
 - (e) the person is detained in custody in a prison; and

Section 46

- (f) there are reasonable grounds to suspect that there is an appreciable risk of the person committing a serious Part 5.3 offence; and
 - (g) consideration is being given, will be given, or is likely to be given, by the AFP Minister (or a person on behalf of the AFP Minister), as to whether to apply for a post-sentence order in relation to the person; and
 - (h) information that would be likely to be obtained by intercepting under a warrant communications made to or from the service would be likely to assist in determining whether to apply for the post-sentence order; and
 - (i) having regard to the matters referred to in subsection (8), and to no other matters, the Judge or nominated AAT member should issue a warrant authorising such communications to be intercepted;
- the Judge or nominated AAT member may, in the Judge's or member's discretion, issue such a warrant.
- (8) For the purposes of subsection (7), the matters to which the Judge or nominated AAT member must have regard are:
- (a) how much the privacy of any person or persons would be likely to be interfered with by intercepting under a warrant communications made to or from the service referred to in subsection (7); and
 - (b) how much the information referred to in paragraph (7)(h) would be likely to assist in determining whether to apply for the post-sentence order; and
 - (c) to what extent methods of determining whether to apply for the post-sentence order that do not involve so intercepting communications have been used by, or are available to, the AFP Minister (or a legal representative of the AFP Minister); and
 - (d) how much the use of such methods would be likely to assist in determining whether to apply for the post-sentence order; and

- (e) how much the use of such methods would be likely to prejudice determining whether to apply for the post-sentence order, whether because of delay or for any other reason; and
- (f) in relation to an application by an interception agency of Victoria—any submissions made by the Victorian PIM under section 44A to the Judge or nominated AAT member; and
- (g) in relation to an application by an interception agency of Queensland—any submissions made by the Queensland PIM under section 45 to the Judge or nominated AAT member.

46A Issue of named person warrant

Warrant relating to the investigation of one or more serious offences

- (1) Where an agency applies to an eligible Judge or nominated AAT member for a warrant in respect of a person and the Judge or nominated AAT member is satisfied, on the basis of the information given to the Judge or nominated AAT member under this Part in connection with the application, that:
 - (a) Division 3 has been complied with in relation to the application; and
 - (b) in the case of a telephone application—because of urgent circumstances, it was necessary to make the application by telephone; and
 - (c) there are reasonable grounds for suspecting that a particular person is using, or is likely to use, more than one telecommunications service; and
 - (d) information that would be likely to be obtained by intercepting under a warrant:
 - (i) communications made to or from any telecommunications service that the person is using, or is likely to use; or
 - (ii) communications made by means of a particular telecommunications device or particular telecommunications devices that the person is using, or is likely to use;

Section 46A

would be likely to assist in connection with the investigation by the agency of a serious offence, or serious offences, in which the person is involved; and

- (e) having regard to the matters referred to in subsection (2), and to no other matters, the Judge or nominated AAT member should issue a warrant authorising such communications to be intercepted;

the Judge or nominated AAT member may, in his or her discretion, issue such a warrant.

Note: Subsection (3) restricts the issuing of a warrant authorising interception of communications made by means of a telecommunications device or telecommunications devices identified in the warrant.

- (2) For the purposes of subsection (1), the matters to which the Judge or nominated AAT member must have regard are:
- (a) how much the privacy of any person or persons would be likely to be interfered with by intercepting under a warrant:
 - (i) communications made to or from any telecommunications service used, or likely to be used, by the person in respect of whom the warrant is sought; or
 - (ii) communications made by means of a particular telecommunications device or particular telecommunications devices used, or likely to be used, by the person in respect of whom the warrant is sought;as the case requires; and
 - (b) the gravity of the conduct constituting the offence or offences being investigated; and
 - (c) how much the information referred to in paragraph (1)(d) would be likely to assist in connection with the investigation by the agency of the offence or offences; and
 - (d) to what extent methods (including the use of a warrant issued under section 46) of investigating the offence or offences that do not involve the use of a warrant issued under this section in relation to the person have been used by, or are available to, the agency; and

- (e) how much the use of such methods would be likely to assist in connection with the investigation by the agency of the offence or offences; and
- (f) how much the use of such methods would be likely to prejudice the investigation by the agency of the offence or offences, whether because of delay or for any other reason; and
- (fa) in relation to an application by an interception agency of Victoria—any submissions made by the Victorian PIM under section 44A to the Judge or nominated AAT member; and
- (g) in relation to an application by an interception agency of Queensland—any submissions made by the Queensland PIM under section 45 to the Judge or nominated AAT member.

Warrant for Part 5.3 supervisory order

- (2A) If a Part 5.3 warrant agency applies to an eligible Judge or nominated AAT member for a warrant in respect of a person and the Judge or nominated AAT member is satisfied, on the basis of the information given to the Judge or nominated AAT member under this Part in connection with the application, that:
 - (a) Division 3 has been complied with in relation to the application; and
 - (b) in the case of a telephone application—because of urgent circumstances, it was necessary to make the application by telephone; and
 - (c) there are reasonable grounds for suspecting that a particular person is using, or is likely to use, more than one telecommunications service; and
 - (d) a Part 5.3 supervisory order is in force in relation to the person; and
 - (e) information that would be likely to be obtained by intercepting under a warrant:
 - (i) communications made to or from any telecommunications service that the person is using, or is likely to use; or

Section 46A

- (ii) communications made by means of a particular telecommunications device or particular telecommunications devices that the person is using, or is likely to use;

would be likely to substantially assist in connection with:

- (iii) achieving a Part 5.3 object; or
- (iv) determining whether the Part 5.3 supervisory order, or any succeeding Part 5.3 supervisory order, has been, or is being, complied with; and

- (f) having regard to the matters referred to in subsection (2B), and to no other matters, the Judge or nominated AAT member should issue a warrant authorising such communications to be intercepted;

the Judge or nominated AAT member may, in his or her discretion, issue such a warrant.

Note 1: Subsection (3) restricts the issuing of a warrant authorising interception of communications made by means of a telecommunications device or telecommunications devices identified in the warrant.

Note 2: For Part 5.3 supervisory orders that have been made but not come into force, see section 6T.

- (2B) For the purposes of subsection (2A), the matters to which the Judge or nominated AAT member must have regard are:

- (a) how much the privacy of any person or persons would be likely to be interfered with by intercepting under a warrant:
 - (i) communications made to or from any telecommunications service used, or likely to be used, by the person in respect of whom the warrant is sought; or
 - (ii) communications made by means of a particular telecommunications device or particular telecommunications devices used, or likely to be used, by the person in respect of whom the warrant is sought; as the case requires; and
- (b) how much the information referred to in paragraph (2A)(e) would be likely to assist in connection with:

- (i) achieving a Part 5.3 object; or
 - (ii) determining whether the Part 5.3 supervisory order, or any succeeding Part 5.3 supervisory order, has been, or is being, complied with; and
- (c) to what extent methods (including the use of a warrant issued under section 46) for:
- (i) achieving a Part 5.3 object; or
 - (ii) determining whether the Part 5.3 supervisory order, or any succeeding Part 5.3 supervisory order, has been, or is being, complied with;
- that do not involve the use of a warrant issued under this section in relation to the person have been used by, or are available to, the agency; and
- (d) how much the use of such methods would be likely to assist in connection with:
- (i) achieving a Part 5.3 object; or
 - (ii) determining whether the Part 5.3 supervisory order, or any succeeding Part 5.3 supervisory order, has been, or is being, complied with; and
- (e) how much the use of such methods would be likely to prejudice:
- (i) achieving a Part 5.3 object; or
 - (ii) determining whether the Part 5.3 supervisory order, or any succeeding Part 5.3 supervisory order, has been, or is being, complied with;
- whether because of delay or for any other reason; and
- (f) whether intercepting under a warrant communications referred to in paragraph (a) of this subsection would be the method that is likely to have the least interference with any person's privacy; and
- (g) in relation to a Part 5.3 supervisory order that is a control order—the possibility that the person in relation to whom the order is in force:
- (i) has engaged, is engaging, or will engage, in a terrorist act; or

Section 46A

- (ii) has provided, is providing, or will provide, support for a terrorist act; or
 - (iii) has facilitated, is facilitating, or will facilitate, a terrorist act; or
 - (iv) has provided, is providing, or will provide, support for the engagement in a hostile activity in a foreign country; or
 - (v) has facilitated, is facilitating, or will facilitate, the engagement in a hostile activity in a foreign country; and
- (ga) in relation to a Part 5.3 supervisory order that is an extended supervision order or interim supervision order—the possibility that the person in relation to whom the order is in force has committed, is committing, or will commit a serious Part 5.3 offence; and
 - (gb) in relation to any Part 5.3 supervisory order—the possibility that the person in relation to whom the order is in force:
 - (i) has contravened, is contravening, or will contravene, the Part 5.3 supervisory order; or
 - (ii) will contravene a succeeding Part 5.3 supervisory order; and
 - (h) in relation to an application by an interception agency of Victoria—any submissions made by the Victorian PIM under section 44A to the Judge or nominated AAT member; and
 - (i) in relation to an application by an interception agency of Queensland—any submissions made by the Queensland PIM under section 45 to the Judge or nominated AAT member.

Warrant sought for post-sentence order application

- (2C) If a Part 5.3 warrant agency applies to an eligible Judge or nominated AAT member for a warrant in respect of a person and the Judge or nominated AAT member is satisfied, on the basis of the information given to the Judge or nominated AAT member under this Part in connection with the application, that:
 - (a) Division 3 has been complied with in relation to the application; and

- (b) in the case of a telephone application—because of urgent circumstances, it was necessary to make the application by telephone; and
 - (c) there are reasonable grounds for suspecting that a particular person is using, or is likely to use, more than one telecommunications service; and
 - (d) the person is a terrorist offender in relation to whom an application for a post-sentence order could be made; and
 - (e) the person is detained in custody in a prison; and
 - (f) there are reasonable grounds to suspect that there is an appreciable risk of the person committing a serious Part 5.3 offence; and
 - (g) consideration is being given, will be given, or is likely to be given, by the AFP Minister (or a person on behalf of the AFP Minister), as to whether to apply for a post-sentence order in relation to the person; and
 - (h) information that would be likely to be obtained by intercepting under a warrant:
 - (i) communications made to or from any telecommunications service that the person is using, or is likely to use; or
 - (ii) communications made by means of a particular telecommunications device or particular telecommunications devices that the person is using, or is likely to use;would be likely to assist in determining whether to apply for the post-sentence order; and
 - (i) having regard to the matters referred to in subsection (2D), and to no other matters, the Judge or nominated AAT member should issue a warrant authorising such communications to be intercepted;
- the Judge or nominated AAT member may, in the Judge's or member's discretion, issue such a warrant.
- (2D) For the purposes of subsection (2C), the matters to which the Judge or nominated AAT member must have regard are:

Section 46A

- (a) how much the privacy of any person or persons would be likely to be interfered with by intercepting under a warrant:
 - (i) communications made to or from any telecommunications service used, or likely to be used, by the person in respect of whom the warrant is sought; or
 - (ii) communications made by means of a particular telecommunications device or particular telecommunications devices used, or likely to be used, by the person in respect of whom the warrant is sought; and
- (b) how much the information referred to in paragraph (2C)(h) would be likely to assist in connection with determining whether to apply for the post-sentence order; and
- (c) to what extent methods (including the use of a warrant issued under section 46) for determining whether to apply for a post-sentence order that do not involve so intercepting communications have been used by, or are available to, the AFP Minister (or a legal representative of the AFP Minister); and
- (d) how much the use of such methods would be likely to assist in determining whether to apply for the post-sentence order; and
- (e) how much the use of such methods would be likely to prejudice determining whether to apply for the post-sentence order, whether because of delay or for any other reasons; and
- (f) in relation to an application by an interception agency of Victoria—any submissions made by the Victorian PIM under section 44A to the Judge or nominated AAT member; and
- (g) in relation to an application by an interception agency of Queensland—any submissions made by the Queensland PIM under section 45 to the Judge or nominated AAT member.

Restriction on issue of warrant—interception of communications made by means of one or more telecommunications devices

- (3) The Judge or nominated AAT member must not issue a warrant that authorises interception of communications made by means of a telecommunications device or telecommunications devices identified in the warrant unless he or she is satisfied that:
- (a) there are no other practicable methods available to the agency at the time of making the application to identify the telecommunications services used, or likely to be used, by the person in respect of whom the warrant would be issued; or
 - (b) interception of communications made to or from a telecommunications service used, or likely to be used, by that person would not otherwise be practicable.

47 Limit on authority conferred by warrant

A warrant issued under section 46 or 46A does not authorise the interception of communications passing over a telecommunications system that a carrier operates unless:

- (a) notification of the issue of the warrant has been received by an authorised representative of the carrier under subsection 60(1); and
- (b) the interception takes place as a result of action taken by an employee of the carrier.

48 Issue of warrant for entry on premises

- (1) If an agency could apply for a warrant under section 46 (authorising interceptions of communications to or from a service), it may instead apply for a warrant under this section that also authorises entry on premises. The agency does so by including in the application that would otherwise have been made under section 46 a request that the warrant also authorise entry on specified premises.

Note: Only a Part 5.3 warrant agency may apply for a warrant under section 46 in the circumstances mentioned in subsection 46(4) or (7).

Section 48

- (2) Where a written application for a warrant includes a request that the warrant authorise entry on specified premises, an affidavit accompanying the application shall:
- (a) state why it is considered necessary for the warrant to authorise entry on those premises;
 - (b) set out the number of previous applications (if any) for warrants that the agency has made and that requested authorisation of entry on those premises; and
 - (c) set out the number of warrants (if any) previously issued on such application.
- (3) Where:
- (a) an agency applies under this section to an eligible Judge or nominated AAT member for a warrant in respect of a telecommunications service; and
 - (b) the Judge or nominated AAT member is satisfied that subsection (2) has been complied with in relation to the application; and
 - (c) section 46 would empower the Judge or nominated AAT member to issue a warrant if the application had been made under either of those sections; and
 - (ca) Division 3 has been complied with in relation to the application; and
 - (d) the Judge or nominated AAT member is satisfied, on the basis of the information given to the Judge or nominated AAT member under this Part in connection with the application, that:
 - (i) for technical reasons connected with the nature or operation of the service or of a telecommunications system of which the service forms a part; or
 - (ii) where, if the warrant were issued under section 46, communications to or from the telecommunications service would be intercepted while passing over a telecommunications system operated by a carrier—execution of the warrant as a result of action taken by employees of that carrier might jeopardise security of the investigation by the agency of a serious offence in

which a person to whom the application relates is involved or, in the case of a warrant issued in the circumstances mentioned in subsection 46(4), might jeopardise the achievement of an objective for which the warrant was issued;

it would be impracticable or inappropriate to intercept communications under a warrant in respect of the service otherwise than by the use of equipment or a line installed on those premises;

subsections (4) and (5) apply.

- (4) The Judge or nominated AAT member may issue a warrant under this section authorising:
 - (a) entry on those premises in order to install, maintain, use or recover equipment or a line used in the interception of communications being made to or from the service; and
 - (b) interceptions of such communications by the use of that equipment or line.

- (5) If the Judge or nominated AAT member issues such a warrant:
 - (a) the warrant shall state whether entry is authorised to be made at any time of the day or night or only during specified hours; and
 - (b) the warrant may provide that entry may be made without permission first being sought or demand first being made, and authorise measures that the Judge or nominated AAT member is satisfied are necessary and reasonable for that purpose.

49 Form and content of warrant

- (1) A warrant shall be in accordance with the prescribed form and shall be signed by the Judge or nominated AAT member who issues it.

- (2) A warrant may specify conditions or restrictions relating to interceptions under the warrant.

Section 49

- (2A) Without limiting subsection (2), a named person warrant may state that the warrant does not authorise the interception of communications made to or from a specified telecommunications service.

Period of warrant

- (3) A warrant shall specify, as the period for which it is to be in force, a period of:
- (a) if subparagraph 46(1)(d)(ii) or 46(4)(d)(ii) applies—up to 45 days; or
 - (b) otherwise—up to 90 days.
- (4) A Judge or nominated AAT member shall not vary a warrant by extending the period for which it is to be in force.
- (5) Neither of subsections (3) and (4) prevents the issue of a further warrant in respect of a service, or a person, in respect of which a warrant has, or warrants have, previously been issued.
- (6) In subsection (5), **warrant** means a warrant issued under this Act.
- (6A) To avoid doubt, a warrant issued on the basis that a Part 5.3 supervisory order is in force remains in force for the period mentioned in subsection (3) even if the order ceases to be in force, provided that the order is replaced by a succeeding Part 5.3 supervisory order.

Note 1: If there is no succeeding Part 5.3 supervisory order, the warrant must be revoked (see section 57).

Note 2: A control order is not a succeeding Part 5.3 supervisory order in relation to an extended supervision order, and vice versa (see section 6U).

Particulars of serious offences

- (7) A warrant issued under subsection 46(1) or 46A(1), or issued under section 48 in the circumstances mentioned in subsection 46(1), shall set out short particulars of each serious offence in relation to

which the Judge or nominated AAT member issuing the warrant was satisfied, on the application for the warrant, as mentioned in:

- (a) in the case of a warrant under section 48—
paragraph 46(1)(d); or
- (b) otherwise—paragraph 46(1)(d) or 46A(1)(d), as the case requires.

Content of warrants issued for Part 5.3 supervisory orders

- (8) A warrant issued for a Part 5.3 supervisory order that is in force must:
 - (a) state that the warrant is issued on the basis of a Part 5.3 supervisory order made in relation to a person; and
 - (b) specify the name of the person; and
 - (c) specify the date the Part 5.3 supervisory order was made; and
 - (d) state whether the Part 5.3 supervisory order is:
 - (i) an interim control order; or
 - (ii) a confirmed control order; or
 - (iii) an interim supervision order; or
 - (iv) an extended supervision order.

Warrants issued for post-sentence order applications

- (9) A warrant issued to determine whether to make an application for a post-sentence order in relation to a person must:
 - (a) state that the warrant is issued on that basis; and
 - (b) specify the name of the person.

50 Issue of warrant on telephone application

- (1) As soon as practicable after completing and signing a warrant issued on a telephone application, a Judge or nominated AAT member shall:
 - (b) inform the person who made the application on the agency's behalf of:
 - (i) the terms of the warrant; and

Section 51

- (ii) the day on which, and the time at which, the warrant was signed; and
 - (c) give the warrant to that person.
- (2) A Judge or nominated AAT member who issues a warrant on a telephone application shall keep a copy of the warrant.

51 Action by agency after warrant issued on telephone application

- (1) A person (in this section called the *applicant*) who makes a telephone application on an agency's behalf shall comply with this section within one day after the day on which a warrant is issued on the application.
- (2) The applicant shall cause each person who gave information to the Judge or nominated AAT member in connection with the application to swear an affidavit setting out the information so given by the person.
- (3) The applicant shall give to the Judge or nominated AAT member:
- (a) the affidavit or affidavits; and
 - (b) unless the applicant is the chief officer of the agency—a copy of an authorisation by the chief officer under subsection 40(3) that was in force in relation to the applicant when the application was made.

52 Judge or nominated AAT member may revoke warrant where section 51 contravened

- (1) Where a Judge or nominated AAT member who issued a warrant on a telephone application is satisfied that section 51 has not been complied with in relation to the warrant, he or she may, by writing signed by him or her, revoke the warrant and shall, if he or she does so:
- (a) immediately inform:
 - (i) the person who made the application on the agency's behalf; or
 - (ii) the chief officer of the agency;

- of the revocation; and
- (b) give the instrument of revocation to that person, or to the chief officer, as soon as practicable.
- (2) Where a warrant issued to an agency is revoked under subsection (1), the chief officer of the agency must, as soon as practicable, give a copy of the instrument of revocation to the Secretary of the Department.
- (3) If:
- (a) a warrant has been issued to an agency; and
 - (b) another agency or the Organisation is exercising authority under that warrant (see section 55); and
 - (c) the warrant is revoked under subsection (1);
- the chief officer of the agency to which the warrant was issued must:
- (d) immediately inform the chief officer of the other agency or the Director-General of Security (as the case requires) of the revocation; and
 - (e) give a copy of the instrument of revocation to the person referred to in paragraph (d) as soon as practicable.

54 Entry into force of warrants

A warrant comes into force when it is issued.

55 Exercise of authority conferred by warrant

- (1) The authority conferred by a Part 2-5 warrant may only be exercised by a person in relation to whom an approval under subsection (3) is in force in relation to the warrant.
- (3) The chief officer of an agency, or an officer of an agency in relation to whom an appointment under subsection (4) is in force, may approve any of the following persons to exercise the authority conferred by warrants (or classes of warrants) issued to the agency:
- (a) officers (or classes of officers) of the agency or another agency;

Section 57

- (b) staff members (or classes of staff members) of the agency or another agency;
 - (c) ASIO employees (or classes of ASIO employees);
 - (d) persons assisting the Organisation in the performance of its functions.
- (4) The chief officer of an agency may appoint in writing an officer of the agency to be an approving officer for the purposes of subsection (3).
- (5) In spite of subsection (1), a designated officer, or an employee of a carrier, may provide technical assistance to a person who is exercising the authority conferred by a warrant.
- (6) A reference in subsection (5) to the provision of technical assistance includes a reference to:
- (a) the doing of any act involved in the interception of a communication under a warrant, to the extent that the act is incidental to the doing of an act referred to in paragraph (b); and
 - (b) the doing of any act in connection with:
 - (i) the installation of equipment for the purposes of intercepting a communication in accordance with a warrant; or
 - (ii) the maintenance, testing or use of such equipment; or
 - (iii) the removal of such equipment.
- (7) The chief officer of an agency or a person who is an approving officer for an agency under subsection (4) may, in writing, declare persons to be designated officers for the purposes of subsection (5).
- (8) To avoid doubt, the Organisation exercises authority under a warrant even if a person assisting the Organisation in the performance of its functions, who is not an ASIO employee, is approved to exercise that authority under paragraph (3)(d).

57 Revocation of warrant by chief officer

- (1) The chief officer of an agency:
 - (a) may, at any time, by signed writing, revoke a warrant issued to the agency; and
 - (b) must do so, if he or she is satisfied that the grounds on which the warrant was issued to the agency have ceased to exist.
- (2) If another agency or the Organisation is exercising authority under the warrant, then before revoking the warrant, the chief officer must inform the chief officer of the other agency or the Director-General of Security (as the case requires) of the proposed revocation.
- (3) After revoking the warrant, the chief officer must:
 - (a) if subsection (2) applies—immediately inform the chief officer of the other agency or the Director-General of Security (as the case requires) of the revocation; and
 - (b) in any case—give a copy of the instrument of revocation to the Secretary of the Department as soon as practicable.
- (4) The chief officer of an agency may delegate his or her power under paragraph (1)(a) to a certifying officer of the agency.
- (5) This section does not apply in relation to a warrant that has ceased to be in force.
- (6) For the purposes of the application of subsection (1) to a Part 5.3 supervisory order warrant issued on the ground that a Part 5.3 supervisory order was in force, that ground is taken to have ceased to exist if, and only if, neither that Part 5.3 supervisory order, nor any succeeding Part 5.3 supervisory order, is in force.

58 Discontinuance of interceptions under certain warrants

- (1) The chief officer of an agency must, on the revocation or proposed revocation of a warrant issued to the agency, immediately take such steps as are necessary to ensure that interceptions of communications under the warrant are discontinued.

Section 59

- (2) If the chief officer of an agency or the Director-General of Security is informed under section 57 of the revocation or proposed revocation of a warrant, he or she must immediately take such steps as are necessary to ensure that interceptions of communications under the warrant by the agency or the Organisation (as the case requires) are discontinued.

59 When revocation of certain warrants takes effect

A warrant revoked under subsection 52(1) or 57(1) does not cease to be in force until the instrument of revocation is received by or on behalf of the Secretary of the Department or the warrant expires, whichever happens sooner.

59A Notification to Secretary of the Department

- (1) Where a Part 2-5 warrant is issued to an agency, the chief officer of the agency must cause a copy of the warrant to be given to the Secretary of the Department as soon as practicable.
- (2) Where:
- (a) it is proposed, under a warrant issued under section 46A, to intercept communications made to or from a telecommunications service; and
 - (b) the warrant is not a warrant that authorises interception of communications made by means of a telecommunications device or telecommunications devices identified in the warrant; and
 - (c) the service was not identified in the warrant;
- the chief officer must cause the Secretary of the Department to be given, as soon as practicable, a description in writing of the service sufficient to identify it.

59B Notification to Ombudsman by Commonwealth agencies in relation to Part 5.3 warrants

- (1) Within 6 months after a Part 5.3 warrant is issued in response to an application by a Commonwealth agency, the chief officer of the agency must:
 - (a) notify the Ombudsman that the warrant has been issued; and
 - (b) give to the Ombudsman a copy of the warrant.
- (2) As soon as practicable after an officer of a Commonwealth agency contravenes any of the following conditions, restrictions or provisions, the chief officer of the agency must notify the Ombudsman of the contravention:
 - (a) a condition or restriction specified in the warrant under subsection 49(2);
 - (b) the following provisions, to the extent that they apply to the warrant:
 - (i) paragraph 57(1)(b);
 - (ii) subsection 63(1);
 - (iii) subsection 63(2);
 - (iv) section 79;
 - (c) section 79AA;
 - (d) subsection 103B(4).
- (3) A failure to comply with subsection (1) or (2) does not affect the validity of the warrant.

60 Notification to authorised representative of carrier of issue or revocation of certain warrants

- (1) Where:
 - (a) a warrant (other than a warrant issued under section 48) is issued to an agency; and
 - (b) it is proposed, under the warrant, to intercept communications to or from a telecommunications service while they are passing over a telecommunications system operated by a carrier;

Section 60

a certifying officer of the agency shall cause;

- (c) an authorised representative of that carrier to be informed immediately of the issue of the warrant; and
- (d) a copy of the warrant, certified in writing by a certifying officer of the agency to be a true copy of the warrant, to be given as soon as practicable to that authorised representative.

(3) Where:

- (a) an authorised representative of a carrier has been informed, under subsection (1), of the issue of a warrant; and
- (b) the warrant is revoked;

a certifying officer of the agency to which the warrant was issued shall cause:

- (c) that authorised representative to be informed immediately of the revocation; and
- (d) a copy of the instrument of revocation, certified in writing by a certifying officer of the agency to be a true copy of the instrument, to be given as soon as practicable to that authorised representative.

(4) Where:

- (a) an authorised representative of a carrier has been informed, under subsection (1), of the issue of a named person warrant; and
- (aa) the warrant is not a warrant that authorises interception of communications made by means of a telecommunications device or telecommunications devices identified in the warrant; and
- (b) it is proposed, under the warrant, to intercept communications made to or from a telecommunications service operated by a carrier; and
- (c) the service was not identified in the warrant;

a certifying officer of the agency must cause that authorised representative to be given, as soon as practicable, a description in writing of the service sufficient to identify it.

(4A) Where:

- (a) an authorised representative of a carrier has been informed, under subsection (1), of the issue of a named person warrant; and
 - (b) the warrant is a warrant that authorises interception of communications made by means of a telecommunications device or telecommunications devices identified in the warrant; and
 - (c) it is proposed, under the warrant, to intercept, by means of a telecommunications device, communications made to or from a telecommunications service operated by the carrier; and
 - (d) the device was not identified in the warrant;
- a certifying officer of the agency must cause that authorised representative to be given, as soon as practicable, a description in writing of the device sufficient to identify it.
- (5) Where:
- (a) an authorised representative of a carrier has been informed, under subsection (1) of the issue of a named person warrant; and
 - (b) a certifying officer of that agency is satisfied that the interception of communications made to or from a particular service, or by means of a particular device or particular devices, is no longer required;
- the certifying officer must cause:
- (c) that authorised representative to be informed immediately of the fact; and
 - (d) confirmation in writing of the fact to be given as soon as practicable to that authorised representative.

61 Evidentiary certificates

- (1) The following:
 - (a) the Managing Director of a carrier;
 - (b) the secretary of a carrier;

Section 61

- (c) an employee of a carrier authorised in writing for the purposes of this paragraph by the Managing Director or the secretary of the carrier;
- may issue a written certificate signed by him or her setting out such facts as he or she considers relevant with respect to acts or things done by, or in relation to, employees of the carrier in order to enable a warrant to be executed.
- (2) A document purporting to be a certificate issued under subsection (1) and purporting to be signed by the Managing Director or secretary, or an employee, of a carrier shall be received in evidence in an exempt proceeding without further proof and is, in an exempt proceeding, conclusive evidence of the matters stated in the document.
- (4) A certifying officer of an agency may issue a written certificate signed by him or her setting out such facts as he or she considers relevant with respect to:
- (a) anything done by an officer or staff member of the agency in connection with the execution of a Part 2-5 warrant; or
 - (b) anything done by an officer or staff member of the agency in connection with:
 - (i) the communication by a person to another person of; or
 - (ii) the making use of; or
 - (iii) the making of a record of; or
 - (iv) the custody of a record of; or
 - (v) the giving in evidence of;information obtained by the execution of such a warrant.
- (4A) A certifying person may issue a written certificate signed by him or her setting out such facts as he or she considers relevant with respect to:
- (a) anything done by a person referred to in paragraph 55(3)(c) or (d) in connection with the execution of a Part 2-5 warrant; or
 - (b) anything done by a person referred to in paragraph 55(3)(c) or (d) in connection with:

- (i) the communication by a person to another person of; or
 - (ii) the making use of; or
 - (iii) the making of a record of; or
 - (iv) the custody of a record of; or
 - (v) the giving in evidence of;
- information obtained by the execution of such a warrant.
- (5) A document purporting to be a certificate issued under subsection (4) or (4A) by a certifying officer of an agency, or a certifying person, and to be signed by him or her:
- (a) is to be received in evidence in an exempt proceeding without further proof; and
 - (b) in an exempt proceeding, is prima facie evidence of the matters stated in the document.
- (6) In subsections (1) and (2), a reference to the Managing Director or secretary of a carrier includes a reference to the Managing Director or secretary of a body corporate of which the carrier is a subsidiary.
- (7) For the purposes of this section, the question whether a body corporate is a subsidiary of another body corporate is to be determined in the same manner as the question is determined under the *Corporations Act 2001*.

61A Certified copy of warrant

A document certified in writing by a certifying officer of an agency to be a true copy of a warrant shall be received in evidence in an exempt proceeding as if it were the original warrant.

Part 2-6—Dealing with intercepted information etc.

62 Application of Part

Except so far as the contrary intention appears, this Part applies in relation to:

- (a) information, whether obtained before or after the commencement of this Part;
- (b) an interception, whether before or after that commencement, of a communication; and
- (c) a proceeding, whether begun before or after that commencement.

63 No dealing in intercepted information or interception warrant information

- (1) Subject to this Part and section 299, a person shall not, after the commencement of this Part:
 - (a) communicate to another person, make use of, or make a record of; or
 - (b) give in evidence in a proceeding;lawfully intercepted information or information obtained by intercepting a communication in contravention of subsection 7(1).
- (2) Subject to this Part and section 299, a person must not, after the commencement of this subsection:
 - (a) communicate interception warrant information to another person; or
 - (b) make use of interception warrant information; or
 - (c) make a record of interception warrant information; or
 - (d) give interception warrant information in evidence in a proceeding.

63AA Dealing in interception warrant information for the purposes of Part 2-2, 2-5, 2-7 or 2-8

A person may, for the purposes of Part 2-2, 2-5, 2-7 or 2-8:

- (a) communicate interception warrant information to another person; or
- (b) make use of interception warrant information; or
- (c) make a record of interception warrant information; or
- (d) give interception warrant information in evidence in a proceeding.

63AB Dealing in general computer access intercept information etc.

(1) A person may, for the purposes of doing a thing authorised by a general computer access warrant:

- (a) communicate general computer access intercept information to another person; or
- (b) make use of general computer access intercept information; or
- (c) make a record of general computer access intercept information; or
- (d) give general computer access intercept information in evidence in a proceeding.

(2) A person may:

- (a) communicate general computer access intercept information to another person; or
- (b) make use of general computer access intercept information; or
- (c) make a record of general computer access intercept information;

if the information relates, or appears to relate, to the involvement, or likely involvement, of a person in one or more of the following activities:

- (d) activities that present a significant risk to a person's safety;
- (e) acting for, or on behalf of, a foreign power;

Section 63AB

- (f) activities that are, or are likely to be, a threat to security;
 - (g) activities that pose a risk, or are likely to pose a risk, to the operational security (within the meaning of the *Intelligence Services Act 2001*) of ASIS (within the meaning of that Act);
 - (ga) activities that pose a risk, or are likely to pose a risk, to the operational security (within the ordinary meaning of that expression) of the Organisation or of AGO or ASD (within the meanings of the *Intelligence Services Act 2001*);
 - (h) activities related to the proliferation of weapons of mass destruction or the movement of goods listed from time to time in the Defence and Strategic Goods List (within the meaning of regulation 13E of the *Customs (Prohibited Exports) Regulations 1958*);
 - (i) activities related to a contravention, or an alleged contravention, by a person of a UN sanction enforcement law (within the meaning of the *Charter of the United Nations Act 1945*).
- (3) A person may, in connection with:
- (a) the performance by an Ombudsman official of the Ombudsman official's functions or duties; or
 - (b) the exercise by an Ombudsman official of the Ombudsman official's powers;
- communicate to the Ombudsman official, or make use of, or make a record of, general computer access intercept information.
- (4) An Ombudsman official may, in connection with:
- (a) the performance by the Ombudsman official of the Ombudsman official's functions or duties; or
 - (b) the exercise by the Ombudsman official of the Ombudsman official's powers;
- communicate to another person, or make use of, or make a record of, general computer access intercept information.
- (5) If:
- (a) information was obtained by intercepting a communication passing over a telecommunications system; and

Section 63AC

- (b) the interception was purportedly for the purposes of doing a thing specified in a general computer access warrant; and
 - (c) the interception was not authorised by the general computer access warrant;
- then:
- (d) a person may, in connection with:
 - (i) the performance by an Ombudsman official of the Ombudsman official's functions or duties; or
 - (ii) the exercise by an Ombudsman official of the Ombudsman official's powers;communicate to the Ombudsman official, or make use of, or make a record of, that information; and
 - (e) an Ombudsman official may, in connection with:
 - (i) the performance by the Ombudsman official of the Ombudsman official's functions or duties; or
 - (ii) the exercise by the Ombudsman official of the Ombudsman official's powers;communicate to another person, or make use of, or make a record of, that information.
- (6) Despite subsection 13.3(3) of the *Criminal Code*, in a prosecution for an offence against section 63 of this Act, an Ombudsman official does not bear an evidential burden in relation to the matters in subsection (4) or (5) of this section.

63AC Dealing in ASIO computer access intercept information etc.

- (1) A person may, for the purposes of doing a thing authorised by an ASIO computer access warrant:
 - (a) communicate ASIO computer access intercept information to another person; or
 - (b) make use of ASIO computer access intercept information; or
 - (c) make a record of ASIO computer access intercept information; or
 - (d) give ASIO computer access intercept information in evidence in a proceeding.

Section 63AC

- (2) A person may:
- (a) communicate ASIO computer access intercept information to another person; or
 - (b) make use of ASIO computer access intercept information; or
 - (c) make a record of ASIO computer access intercept information;
- if the information relates, or appears to relate, to the involvement, or likely involvement, of a person in one or more of the following activities:
- (d) activities that present a significant risk to a person's safety;
 - (e) acting for, or on behalf of, a foreign power;
 - (f) activities that are, or are likely to be, a threat to security;
 - (g) activities that pose a risk, or are likely to pose a risk, to the operational security (within the meaning of the *Intelligence Services Act 2001*) of ASIS (within the meaning of that Act);
 - (ga) activities that pose a risk, or are likely to pose a risk, to the operational security (within the ordinary meaning of that expression) of the Organisation or of AGO or ASD (within the meanings of the *Intelligence Services Act 2001*);
 - (h) activities related to the proliferation of weapons of mass destruction or the movement of goods listed from time to time in the Defence and Strategic Goods List (within the meaning of regulation 13E of the *Customs (Prohibited Exports) Regulations 1958*);
 - (i) activities related to a contravention, or an alleged contravention, by a person of a UN sanction enforcement law (within the meaning of the *Charter of the United Nations Act 1945*).
- (3) A person may, in connection with:
- (a) the performance by an IGIS official of the IGIS official's functions or duties; or
 - (b) the exercise by an IGIS official of the IGIS official's powers; communicate to the IGIS official, or make use of, or make a record of, ASIO computer access intercept information.

- (4) An IGIS official may, in connection with:
- (a) the performance by the IGIS official of the IGIS official's functions or duties; or
 - (b) the exercise by the IGIS official of the IGIS official's powers;
- communicate to another person, or make use of, or make a record of, ASIO computer access intercept information.
- (5) If:
- (a) information was obtained by intercepting a communication passing over a telecommunications system; and
 - (b) the interception was purportedly for the purposes of doing a thing specified in an ASIO computer access warrant; and
 - (c) the interception was not authorised by the ASIO computer access warrant;
- then:
- (d) a person may, in connection with:
 - (i) the performance by an IGIS official of the IGIS official's functions or duties; or
 - (ii) the exercise by an IGIS official of the IGIS official's powers;communicate to the IGIS official, or make use of, or make a record of, that information; and
 - (e) an IGIS official may, in connection with:
 - (i) the performance by the IGIS official of the IGIS official's functions or duties; or
 - (ii) the exercise by the IGIS official of the IGIS official's powers;communicate to another person, or make use of, or make a record of, that information.
- (6) Despite subsection 13.3(3) of the *Criminal Code*, in a prosecution for an offence against section 63 of this Act, an IGIS official does not bear an evidential burden in relation to the matters in subsection (4) or (5) of this section.

Section 63AD

63AD Dealing in data disruption intercept information etc.

- (1) A person may, for the purposes of doing a thing authorised by a data disruption warrant:
- (a) communicate data disruption intercept information to another person; or
 - (b) make use of data disruption intercept information; or
 - (c) make a record of data disruption intercept information; or
 - (d) give data disruption intercept information in evidence in a proceeding.
- (2) A person may:
- (a) communicate data disruption intercept information to another person; or
 - (b) make use of data disruption intercept information; or
 - (c) make a record of data disruption intercept information;
- if the information relates, or appears to relate, to the involvement, or likely involvement, of a person in one or more of the following activities:
- (d) activities that present a significant risk to a person's safety;
 - (e) acting for, or on behalf of, a foreign power (within the meaning of the *Australian Security Intelligence Organisation Act 1979*);
 - (f) activities that are, or are likely to be, a threat to security;
 - (g) activities that pose a risk, or are likely to pose a risk, to the operational security (within the meaning of the *Intelligence Services Act 2001*) of ASIS (within the meaning of that Act);
 - (h) activities that pose a risk, or are likely to pose a risk, to the operational security (within the ordinary meaning of that expression) of the Organisation or of AGO or ASD (within the meanings of the *Intelligence Services Act 2001*);
 - (i) activities related to the proliferation of weapons of mass destruction or the movement of goods listed from time to time in the Defence and Strategic Goods List (within the meaning of regulation 13E of the *Customs (Prohibited Exports) Regulations 1958*);

Section 63AD

- (j) activities related to a contravention, or an alleged contravention, by a person of a UN sanction enforcement law (within the meaning of the *Charter of the United Nations Act 1945*).
- (3) A person may, in connection with:
- (a) the performance by an Ombudsman official of the Ombudsman official's functions or duties; or
 - (b) the exercise by an Ombudsman official of the Ombudsman official's powers;
- communicate to the Ombudsman official, or make use of, or make a record of, data disruption intercept information.
- (4) An Ombudsman official may, in connection with:
- (a) the performance by the Ombudsman official of the Ombudsman official's functions or duties; or
 - (b) the exercise by the Ombudsman official of the Ombudsman official's powers;
- communicate to another person, or make use of, or make a record of, data disruption intercept information.
- (5) A person may, in connection with:
- (a) the performance by an IGIS official of the IGIS official's functions or duties; or
 - (b) the exercise by an IGIS official of the IGIS official's powers;
- communicate to the IGIS official, or make use of, or make a record of, data disruption intercept information.
- (6) An IGIS official may, in connection with:
- (a) the performance by the IGIS official of the IGIS official's functions or duties; or
 - (b) the exercise by the IGIS official of the IGIS official's powers;
- communicate to another person, or make use of, or make a record of, data disruption intercept information.
- (7) If:
-

Section 63AD

- (a) information was obtained by intercepting a communication passing over a telecommunications system; and
- (b) the interception was purportedly for the purposes of doing a thing specified in a data disruption warrant; and
- (c) the interception was not authorised by the data disruption warrant;

then:

- (d) a person may, in connection with:
 - (i) the performance by an Ombudsman official of the Ombudsman official's functions or duties; or
 - (ii) the exercise by an Ombudsman official of the Ombudsman official's powers;communicate to the Ombudsman official, or make use of, or make a record of, that information; and
- (e) an Ombudsman official may, in connection with:
 - (i) the performance by the Ombudsman official of the Ombudsman official's functions or duties; or
 - (ii) the exercise by the Ombudsman official of the Ombudsman official's powers;communicate to another person, or make use of, or make a record of, that information; and
- (f) a person may, in connection with:
 - (i) the performance by an IGIS official of the IGIS official's functions or duties; or
 - (ii) the exercise by an IGIS official of the IGIS official's powers;communicate to the IGIS official, or make use of, or make a record of, that information; and
- (g) an IGIS official may, in connection with:
 - (i) the performance by the IGIS official of the IGIS official's functions or duties; or
 - (ii) the exercise by the IGIS official of the IGIS official's powers;communicate to another person, or make use of, or make a record of, that information.

Section 63AE

- (8) Despite subsection 13.3(3) of the *Criminal Code*, in a prosecution for an offence against section 63 of this Act, an Ombudsman official or an IGIS official does not bear an evidential burden in relation to the matters in subsection (4), (6) or (7) of this section.

63AE Dealing in network activity warrant intercept information etc.

- (1) A person may, for the purposes of doing a thing authorised by a network activity warrant:
- (a) communicate network activity warrant intercept information to another person; or
 - (b) make use of network activity warrant intercept information; or
 - (c) make a record of network activity warrant intercept information; or
 - (d) give network activity warrant intercept information in evidence in:
 - (i) a criminal proceeding for an offence against section 105 so far as the offence relates to contravening section 63; or
 - (ii) a proceeding that is not a criminal proceeding.
- (2) A person may:
- (a) communicate network activity warrant intercept information to another person; or
 - (b) make use of network activity warrant intercept information; or
 - (c) make a record of network activity warrant intercept information;
- if the information relates, or appears to relate, to the involvement, or likely involvement, of a person in one or more of the following activities:
- (d) activities that present a significant risk to a person's safety;
 - (e) acting for, or on behalf of, a foreign power (within the meaning of the *Australian Security Intelligence Organisation Act 1979*);

Section 63AE

- (f) activities that are, or are likely to be, a threat to security;
 - (g) activities that pose a risk, or are likely to pose a risk, to the operational security (within the meaning of the *Intelligence Services Act 2001*) of ASIS (within the meaning of that Act);
 - (h) activities that pose a risk, or are likely to pose a risk, to the operational security (within the ordinary meaning of that expression) of the Organisation or of AGO or ASD (within the meanings of the *Intelligence Services Act 2001*);
 - (i) activities related to the proliferation of weapons of mass destruction or the movement of goods listed from time to time in the Defence and Strategic Goods List (within the meaning of regulation 13E of the *Customs (Prohibited Exports) Regulations 1958*);
 - (j) activities related to a contravention, or an alleged contravention, by a person of a UN sanction enforcement law (within the meaning of the *Charter of the United Nations Act 1945*).
- (3) A person may, in connection with:
- (a) the performance by an IGIS official of the IGIS official's functions or duties; or
 - (b) the exercise by an IGIS official of the IGIS official's powers; communicate to the IGIS official, or make use of, or make a record of, network activity warrant intercept information.
- (4) An IGIS official may, in connection with:
- (a) the performance by the IGIS official of the IGIS official's functions or duties; or
 - (b) the exercise by the IGIS official of the IGIS official's powers; communicate to another person, or make use of, or make a record of, network activity warrant intercept information.
- (5) If:
- (a) information was obtained by intercepting a communication passing over a telecommunications system; and

Section 63A

- (b) the interception was purportedly for the purposes of doing a thing specified in a network activity warrant; and
 - (c) the interception was not authorised by the network activity warrant;
- then:
- (d) a person may, in connection with:
 - (i) the performance by an IGIS official of the IGIS official's functions or duties; or
 - (ii) the exercise by an IGIS official of the IGIS official's powers;communicate to the IGIS official, or make use of, or make a record of, that information; and
 - (e) an IGIS official may, in connection with:
 - (i) the performance by the IGIS official of the IGIS official's functions or duties; or
 - (ii) the exercise by the IGIS official of the IGIS official's powers;communicate to another person, or make use of, or make a record of, that information.
- (6) Despite subsection 13.3(3) of the *Criminal Code*, in a prosecution for an offence against section 63 of this Act, an IGIS official does not bear an evidential burden in relation to the matters in subsection (4) or (5) of this section.

63A Dealing in connection with existing proceeding

- (1) A person may:
 - (a) for a purpose connected with a proceeding begun before the commencement of this Part, or for 2 or more such purposes, and for no other purpose, communicate to another person, make use of, or make a record of; or
 - (b) give in evidence in such a proceeding;information:

Section 63B

- (c) obtained by intercepting a communication before that commencement, whether or not in contravention of subsection 7(1); or
 - (d) obtained, before that commencement, by virtue of a warrant issued under section 11A.
- (2) Nothing in subsection (1) makes admissible in evidence in any proceedings information, obtained by virtue of a warrant that was defective, that would not have been admissible in those proceedings if that subsection had not been enacted.
 - (3) For the purposes of this section, a proceeding by way of a prosecution of a person on indictment for an offence shall be deemed to have begun before the commencement of this Part if a proceeding with a view to the committal of the person for trial for the offence began before that commencement.
 - (4) For the purposes of this section, a proceeding by way of an appeal from, or otherwise arising out of, another proceeding shall be deemed to have begun before the commencement of this Part if the other proceeding began, or by virtue of any other application or applications of this section is deemed to have begun, before that commencement.

63B Dealing in information by employees of carriers

- (1) An employee of a carrier may, in the performance of his or her duties as such an employee, communicate or make use of, or cause to be communicated, information (being information that has been lawfully obtained or obtained by intercepting a communication in contravention of subsection 7(1)) relating to:
 - (a) the operation or maintenance of a telecommunications network operated by the carrier; or
 - (b) the supply of services by the carrier by means of a telecommunications network.
- (2) An employee of a carrier may communicate or cause to be communicated to another carrier, or to an employee of another carrier, information (being information that has been lawfully

Section 63B

obtained or obtained by intercepting a communication in contravention of subsection 7(1)) relating to:

- (a) the operation or maintenance of a telecommunications network operated by the other carrier; or
- (b) the supply of services by the other carrier by means of a telecommunications network;

if the communication of the information is for the purpose of the carrying on by the other carrier of its business relating to the supply of services by means of a telecommunications network operated by the other carrier.

- (3) An employee of a carrier may, in the performance of his or her duties as such an employee, communicate or make use of, or cause to be communicated, interception warrant information if the information is reasonably necessary to enable the interception of a communication under a warrant.
- (4) An employee of a carrier may communicate or cause to be communicated to another carrier, or to an employee of another carrier, interception warrant information if the information is reasonably necessary to enable the interception of a communication under a warrant.
- (5) If an employee of a carrier has obtained lawfully intercepted information under a section 31A authorisation that was given in response to an application made by the head (however described) of a security authority or a person acting as that head, the employee may:
 - (a) communicate the information to:
 - (i) an employee of the security authority; or
 - (ii) another employee of the carrier; or
 - (iii) if the authorisation covers the employees of one or more other carriers—an employee of any of those other carriers; or
 - (b) make use of the information; or
 - (c) make a record of the information;if:

Section 63C

- (d) the employee does so for the purposes of the development or testing of technologies, or interception capabilities, to which the authorisation relates; and
- (e) the communication or use of the information, or the making of the record, as the case may be, does not contravene a condition to which the authorisation is subject.

63C Dealing in information for network protection purposes etc.

- (1) Subject to subsection (3), a person engaged in network protection duties in relation to a computer network may, in performing those duties, communicate or make use of, or cause to be communicated, lawfully intercepted information that was obtained by intercepting a communication under paragraph 7(2)(aaa).
- (2) Subject to subsection (3), a person engaged in network protection duties in relation to a computer network may communicate, or cause to be communicated, to the following persons lawfully intercepted information that was obtained by intercepting a communication under paragraph 7(2)(aaa):
 - (a) a responsible person for the network;
 - (b) another person if the information is reasonably necessary to enable the other person to perform the other person's network protection duties in relation to the network.
- (3) A person must not communicate or make use of, or cause to be communicated, lawfully intercepted information under subsection (1) or (2) if the information was obtained by converting a communication intercepted under paragraph 7(2)(aaa) into a voice communication in the form of speech (including a communication that involves a recorded or synthetic voice).

63D Dealing in information for disciplinary purposes

- (1) This section applies to a person engaged in network protection duties in relation to a computer network if:
 - (a) the network is operated by, or on behalf of, a Commonwealth agency, security authority or eligible authority of a State; and

Section 63E

- (b) the duties are of a kind referred to in paragraph (b) of the definition of *network protection duties* in subsection 5(1).
- (2) Subject to subsections (3) and (4), the person may communicate or make use of, or cause to be communicated, lawfully intercepted information that was obtained by intercepting a communication under paragraph 7(2)(aaa) if the communication or use is for the purpose of:
- (a) determining whether disciplinary action should be taken in relation to a use of the network by an employee, office holder or contractor of the agency or authority; or
 - (b) taking disciplinary action in relation to a use of the network by such an employee, office holder or contractor in a case where the use is not an appropriate use of the network by that employee, office holder or contractor; or
 - (c) reviewing a decision to take such disciplinary action.
- Note: See section 6AAA for when a computer network is appropriately used by such an employee, office holder or contractor.
- (3) A person must not communicate or make use of, or cause to be communicated, lawfully intercepted information under subsection (2) if the information was obtained by converting a communication intercepted under paragraph 7(2)(aaa) into a voice communication in the form of speech (including a communication that involves a recorded or synthetic voice).
- (4) A person must not communicate or make use of, or cause to be communicated, lawfully intercepted information for a purpose referred to in subsection (2) if the person would contravene another law of the Commonwealth, or a law of a State or Territory, in doing so.

63E Responsible person for a computer network may communicate information to an agency

A responsible person for a computer network may communicate lawfully intercepted information (other than foreign intelligence information) to an officer of an agency if:

Section 64

- (a) the information was communicated to the responsible person under paragraph 63C(2)(a); and
- (b) the responsible person suspects, on reasonable grounds, that the information is relevant to determining whether another person has committed a prescribed offence.

64 Dealing in connection with Organisation's or Inspector-General's functions

- (1) A person may, in connection with the performance by the Organisation of its functions or the performance by the Inspector-General of Intelligence and Security of his or her functions, or otherwise for purposes of security, communicate to another person, make use of, or make a record of the following:
 - (a) lawfully intercepted information other than foreign intelligence information or ASIO computer access intercept information;
 - (b) interception warrant information.
- (2) A person, being the Director-General of Security or an ASIO employee, ASIO affiliate or IGIS official, may:
 - (a) in connection with the performance by the Organisation of its functions; or
 - (b) in connection with the performance by the Inspector-General of Intelligence and Security of his or her functions;communicate to another such person, make use of, or make a record of, foreign intelligence information.
- (3) Subsections (1) and (2) do not apply to information:
 - (a) obtained by a person referred to in paragraph 55(3)(c) or (d) by intercepting a communication when exercising authority under a warrant issued to an agency; or
 - (b) communicated, in accordance with section 66, to a person referred to in paragraph 55(3)(c); or
 - (c) that is interception warrant information in relation to a warrant issued to an agency;

unless the information has been communicated to the Director-General of Security under section 68.

- (4) However, a person referred to in paragraph 55(3)(c) or (d) may communicate to another person, make use of, or make a record of information referred to in paragraph (3)(a), (b) or (c) of this section, that has not been communicated to the Director-General of Security under section 68, for a purpose or purposes connected with the investigation to which the warrant, under which the information was obtained, relates, and for no other purpose.

65 Dealing in information obtained by Organisation

- (1) The Director-General of Security may, personally, or by a person authorised by the Director-General, communicate to another person, in accordance with subsection 18(3) or (4A), or subsection 19A(4) of the *Australian Security Intelligence Organisation Act 1979* the following:
- (a) lawfully intercepted information other than ASIO computer access intercept information;
 - (b) interception warrant information.
- (2) A person to whom foreign intelligence information has been communicated in accordance with subsection (1), or in accordance with an approval given under this subsection, may:
- (a) communicate that information to such persons, and in such manner, as are approved in writing by the Attorney-General; and
 - (b) use that information for such purposes as are approved in writing by the Attorney-General; and
 - (c) make a record of that information.
- (3) Subsections (1) and (2) do not apply to information:
- (a) obtained by a person referred to in paragraph 55(3)(c) or (d) by intercepting a communication when exercising authority under a warrant issued to an agency; or
 - (b) communicated, in accordance with section 66, to a person referred to in paragraph 55(3)(c); or

Section 65

(c) that is interception warrant information in relation to a warrant issued to an agency;

unless the information has been communicated to the Director-General of Security under section 68.

Note: See subsection 64(4) for when the Director-General of Security may communicate information, referred to in paragraph (3)(a), (b) or (c) of this section, that has not been communicated under section 68.

(4) If lawfully intercepted information was obtained under a section 31A authorisation, subsection (1) of this section does not authorise the communication of the information in accordance with subsection 18(3) of the *Australian Security Intelligence Organisation Act 1979* to:

- (a) a staff member of an authority of the Commonwealth; or
- (b) a staff member of an authority of a State;

unless the communication is for the purpose of the development or testing of technologies, or interception capabilities, of:

- (c) that authority; or
- (d) the Organisation.

(5) If lawfully intercepted information was obtained under a section 31A authorisation, subsection (1) of this section does not authorise the communication of the information in accordance with subsection 18(4A) of the *Australian Security Intelligence Organisation Act 1979* to a staff member of ASIS, ASD or AGO unless the communication is for the purpose of the development or testing of technologies, or interception capabilities, of:

- (a) ASIS, ASD or AGO, as the case requires; or
- (b) the Organisation.

(6) If lawfully intercepted information was obtained under a section 31A authorisation, subsection (1) of this section does not authorise the communication of the information in accordance with subsection 19A(4) of the *Australian Security Intelligence Organisation Act 1979* to a staff member of a body referred to in paragraph 19A(1)(d) or (e) of that Act unless the communication is for the purpose of the development or testing of technologies, or interception capabilities, of:

- (a) that body; or
 - (b) the Organisation.
- (6A) An approval under subsection (2) is not a legislative instrument.
- (7) For the purposes of subsections (4), (5) and (6), **authority of the Commonwealth, authority of a State, ASIS, ASD, AGO** and **staff member** have the same respective meanings as in the *Australian Security Intelligence Organisation Act 1979*.

65A Employee of carrier may communicate information to agency

- (1) An employee of a carrier may, for a purpose or purposes set out in subsection (2), and for no other purpose, communicate to an officer of an agency:
- (a) lawfully intercepted information other than foreign intelligence information or information obtained under a section 31A authorisation; or
 - (b) interception warrant information.
- (2) The purposes are purposes connected with:
- (a) the investigation by the agency of a serious offence; or
 - (b) any of the following:
 - (i) achieving a Part 5.3 object;
 - (ii) determining whether a Part 5.3 supervisory order has been, or is being, complied with;
 - (v) the performance of a function or duty, or the exercise of a power, by a person, court or other body under, or in relation to a matter arising under, Division 104 (control orders) or Division 105A (post-sentence orders) of the *Criminal Code*;
 - (vi) a preventative detention order law;
 - (vii) the performance of a function or duty, or the exercise of a power, by a person, court or other body under, or in relation to a matter arising under, a post-sentence detention law or a post-sentence supervision law.

Section 66

66 Interceptor may communicate to officer who applied for warrant or authorised person

- (1) A person who has intercepted a communication under a warrant issued to an agency may communicate information obtained by the interception to:
 - (a) the officer of the agency who applied for the warrant on the agency's behalf; or
 - (b) a person in relation to whom an authorisation under subsection (2) is in force in relation to the warrant.
- (2) The chief officer of an agency, or an authorising officer of an agency for whom an appointment under subsection (4) is in force, may authorise in writing a person (or class of person) referred to in any of paragraphs 55(3)(a) to (c) to receive information obtained by interceptions under warrants (or classes of warrants) issued to the agency.
- (3) The chief officer, or an authorising officer, of an agency may make an authorisation under subsection (2) in relation to a person (or class of person) who is not an officer or staff member of that agency only for a purpose or purposes connected with an investigation to which a warrant issued to that agency relates.
- (4) The chief officer of an agency may appoint in writing an officer of the agency to be an authorising officer for the purposes of this section.

67 Dealing for permitted purposes

Dealing for permitted purposes in relation to an agency

- (1) An officer or staff member of an agency may, for a permitted purpose, or permitted purposes, in relation to the agency, and for no other purpose, communicate to another person, make use of, or make a record of the following:
 - (a) lawfully intercepted information other than foreign intelligence information, general computer access intercept

information, data disruption intercept information or network activity warrant intercept information;

(b) interception warrant information.

(1A) Subsection (1) does not apply to information:

- (a) obtained by an officer or staff member of an agency by intercepting a communication when exercising authority under a warrant issued to another agency; or
- (b) communicated to an officer or staff member of an agency in accordance with section 66, where the information was obtained by intercepting a communication under a warrant issued to another agency; or
- (c) that is interception warrant information in relation to a warrant issued to another agency;

unless the information has been communicated to an officer of the agency under section 68.

(1B) However, an officer or staff member of an agency may communicate to another person, make use of, or make a record of information mentioned in paragraph (1A)(a), (b) or (c) for a purpose or purposes set out in subsection (1C), and for no other purpose, if the information has not been communicated to an officer of the agency under section 68.

(1C) The purposes are purposes connected with:

- (a) if the warrant under which the information was obtained relates to an investigation—the investigation; or
- (b) if the information was obtained under a Part 5.3 warrant issued on the basis that a Part 5.3 supervisory order was in force in relation to a person—any of the following:
 - (i) achieving a Part 5.3 object;
 - (ii) determining whether the Part 5.3 supervisory order has been, or is being, complied with; or
- (c) if the information was obtained under any Part 5.3 warrant—the performance of a function or duty, or the exercise of a power, by a person, court or other body under, or in relation to a matter arising under:

Section 68

- (i) Division 104 (control orders) or Division 105A (post-sentence orders) of the *Criminal Code*; or
- (ii) a post-sentence detention order or a post-sentence supervision order; or
- (iii) a preventative detention order law.

Dealing for permitted purposes in relation to an eligible Commonwealth authority

- (2) An officer of an eligible Commonwealth authority may, for a permitted purpose, or permitted purposes, in relation to the authority, and for no other purpose, communicate to another person, make use of, or make a record of the following:
 - (a) lawfully intercepted information other than foreign intelligence information;
 - (b) interception warrant information.

Dealing for permitted purposes in relation to ASIC

- (3) A member of ASIC or a staff member of ASIC may, for a permitted purpose, or permitted purposes, in relation to ASIC, and for no other purpose, communicate to another person, make use of, or make a record of the following:
 - (a) lawfully intercepted information other than foreign intelligence information;
 - (b) interception warrant information.

68 Chief officer may communicate information obtained by agency

The chief officer of an agency (in this section called the **originating agency**) may, personally, or by an officer of the originating agency authorised by the chief officer, communicate lawfully intercepted information (other than general computer access intercept information, data disruption intercept information or network activity warrant intercept information) that was originally obtained by the originating agency or interception warrant information:

- (a) if the information relates, or appears to relate, to activities prejudicial to security—to the Director-General of Security; and
- (b) if the information relates, or appears to relate, to the commission of a relevant offence in relation to another agency:
 - (i) if the other agency is the Australian Federal Police or the Police Force of a State—to a member of the Australian Federal Police or an officer of that Police Force, as the case may be; or
 - (ii) in any other case—to the chief officer of the other agency; and
- (c) if the information relates, or appears to relate, to:
 - (i) the subject matter of a proceeding under a law of the Commonwealth for the confiscation or forfeiture of property, or for the imposition of a pecuniary penalty, in connection with the commission of a prescribed offence; or
 - (ia) the subject matter of a proceeding under, or in relation to a matter arising under, the main unexplained wealth provisions; or
 - (ii) an act or omission by a member of the Australian Federal Police that may give rise to a proceeding against that member, or to which a proceeding against that member relates, being a police disciplinary proceeding; or
 - (iia) an act or omission by an AFP employee or special member of the Australian Federal Police that may give rise to a decision by the Commissioner of Police to terminate the employment of the employee or the appointment of the special member; or
 - (iii) misbehaviour or improper conduct of an officer of the Commonwealth;and the originating agency is not the Australian Federal Police—to the Commissioner of Police; and
- (ca) if:

Section 68

- (i) the information relates, or appears to relate, to an act or omission by a member of the staff of the ACC that may give rise to a decision by the Chief Executive Officer of the ACC to terminate the employment of the staff member; and
- (ii) the originating agency is not the ACC;
to the Chief Executive Officer of the ACC; and
- (d) if the information relates, or appears to relate, to:
 - (i) the subject matter of a proceeding under a law of a State for the confiscation or forfeiture of property, or for the imposition of a pecuniary penalty, in connection with the commission of a prescribed offence; or
 - (iaa) the subject matter of a proceeding under, or in relation to a matter arising under, the unexplained wealth legislation of a participating State, the Australian Capital Territory or the Northern Territory; or
 - (ia) the subject matter of a proceeding under, or in relation to a matter arising under, an organised crime control law of a State; or
 - (ii) an act or omission by an officer of the Police Force of a State that may give rise to a proceeding against that officer, or to which a proceeding against that officer relates, being a police disciplinary proceeding; or
 - (iia) an act or omission by an officer or member of staff of the Police Force of a State that may give rise to a decision by the Commissioner of that Police Force to terminate the appointment of the officer or member of staff; or
 - (iii) misbehaviour or improper conduct of an officer of a State;
and the originating agency is not the Police Force of that State—to the Commissioner of that Police Force; and
- (da) if the information relates, or appears to relate, to the commission of a relevant offence in relation to an eligible Commonwealth authority—to the chief officer of the eligible Commonwealth authority; and

- (db) if the information relates, or appears to relate, to a corruption issue or an ACLEI corruption issue (within the meaning of the *Law Enforcement Integrity Commissioner Act 2006*)—to the Integrity Commissioner; and
- (ea) if the information relates, or appears to relate, to a matter that may give rise to an investigation by the Independent Commission Against Corruption—to the Chief Commissioner of the Independent Commission Against Corruption; and
- (eb) if the information relates, or appears to relate, to a matter that may give rise to an investigation by the Inspector of the Independent Commission Against Corruption—to the Inspector of the Independent Commission Against Corruption; and
- (ec) if the information relates, or appears to relate, to a matter that may give rise to an investigation by the IBAC—to the Commissioner of the IBAC; and
- (ed) if the information relates, or appears to relate, to a matter that may give rise to an investigation by the Victorian Inspectorate—to the Inspector of the Victorian Inspectorate; and
- (f) if the information relates, or appears to relate, to a matter that may give rise to an investigation by the Law Enforcement Conduct Commission—to the Chief Commissioner of the Commission; and
- (fa) if the information relates, or appears to relate, to a matter that may give rise to an investigation by the Inspector of the Law Enforcement Conduct Commission—to the Inspector; and
- (h) if the information relates, or appears to relate, to a matter that may give rise to an investigation by the Crime and Corruption Commission—to the Commissioner of the Crime and Corruption Commission; and
- (j) if the information relates, or appears to relate, to a matter that may give rise to an investigation by the Corruption and Crime Commission—to the Commissioner of the Corruption and Crime Commission; and

Section 68

- (ja) if the information relates, or appears to relate, to a matter that may give rise to an investigation by the Independent Commissioner Against Corruption—to the Independent Commissioner Against Corruption; and
- (k) if the information relates, or appears to relate, to a matter that may give rise to the dealing by the Parliamentary Inspector of the Corruption and Crime Commission with a matter of misconduct (within the meaning of the Corruption and Crime Commission Act)—to the Parliamentary Inspector of the Corruption and Crime Commission; and
- (l) if the Attorney-General has authorised the provision of the information to a foreign country under subsection 13A(1) of the *Mutual Assistance in Criminal Matters Act 1987*—to that foreign country, or to the Secretary of the Department administered by that Minister for the purpose of providing the information to that foreign country; and
- (la) if the Attorney-General has authorised the provision of the information to the International Criminal Court under section 69A of the *International Criminal Court Act 2002*—to:
 - (i) that Court; or
 - (ii) the Secretary of the Department administered by that Minister for the purpose of providing the information to that Court; and
- (lb) if the Attorney-General has authorised the provision of the information to a War Crimes Tribunal under section 25A of the *International War Crimes Tribunals Act 1995*—to:
 - (i) that Tribunal; or
 - (ii) the Secretary of the Department administered by that Minister for the purpose of providing the information to that Tribunal; and
- (m) to the chief officer of the Australian Federal Police or the ACC, if the information relates, or appears to relate, to either of the following:

- (i) a matter in relation to which an application for an integrity authority may be made, is intended to be made or has been made in relation to that agency;
- (ii) a matter in relation to which that agency has conducted, or is conducting, an integrity operation; and
- (n) to the chief officer of the Australian Commission for Law Enforcement Integrity, if the information relates, or appears to relate, to either of the following:
 - (i) a matter in relation to which an application for an integrity authority may be made, is intended to be made or has been made in relation to the Australian Federal Police, the ACC or the Immigration and Border Protection Department;
 - (ii) a matter in relation to which the Australian Commission for Law Enforcement Integrity has conducted, or is conducting, an integrity operation; and
- (o) if the originating agency is the Australian Commission for Law Enforcement Integrity—to the Secretary of the Immigration and Border Protection Department, in the case of information that relates, or appears to relate, to either of the following:
 - (i) a matter in relation to which an application for an integrity authority may be made, is intended to be made or has been made in relation to the Immigration and Border Protection Department;
 - (ii) a matter in relation to which the Immigration and Border Protection Department is conducting an integrity operation; and
- (p) to a member of ASIC or a staff member of ASIC, if the information relates, or appears to relate, to a matter that may give rise to an investigation by ASIC of:
 - (i) a serious offence; or
 - (ii) the likely commission of a serious offence.

Section 68A

68A Communicating information obtained by the Secretary of the Attorney-General's Department

- (1) This section applies to information communicated to the Secretary of the Department administered by the Attorney-General as described in an item of the following table:

Information to which this section applies		
Item	Information communicated under this provision:	For the purpose of providing it to this entity:
1	paragraph 68(l)	the foreign country concerned
2	paragraph 68(la)	the International Criminal Court
3	paragraph 68(lb)	the War Crimes Tribunal concerned

- (2) Each of the following:
- (a) the Secretary of that Department;
 - (b) a person authorised by that Secretary;
 - (c) a person or other entity to whom the information has been communicated under this subsection;
- may communicate the information to another person or entity for purposes connected with providing the information to the entity mentioned in that table item.

69 State authority may ask not to receive information under section 68

- (1) The chief officer of an eligible authority of a State in relation to which no declaration is in force under section 34 may, by writing given to the chief officer of another agency, request the other agency not to communicate information under section 68 to the eligible authority.
- (2) A request under subsection (1) remains in force until:
- (a) the chief officer of the eligible authority revokes the request by writing given to the chief officer of the other agency; or

- (b) a declaration is made under section 34 in relation to the eligible authority.
- (3) Where a request under subsection (1) is in force, section 68 does not permit an officer of the other agency to communicate information to an officer of the eligible authority.

70 Communicating information obtained by interception under Part 2-3

A member of a police force may, in the course of performing his or her duties as such a member, communicate to another member of a police force, or to any other person whose assistance may be required in dealing with an emergency of a kind referred to in paragraph 30(1)(b), information communicated (whether before or after the commencement of this section) to the first-mentioned member in accordance with subsection 30(3) or this section.

71 Dealing with information where interception suspected to be unlawful

- (1) Where a person suspects on reasonable grounds that information (in this section called the *relevant information*) obtained by intercepting a communication may tend to establish that a prescribed offence (in this section called a *suspected offence*), being:
 - (a) an offence against subsection 7(1) constituted by the interception, or by authorising, suffering or permitting, or doing an act or thing to enable, the interception;
 - (b) an offence against section 63 constituted by communicating to a person, making use of, making a record of, or giving in evidence in a proceeding, information obtained by the interception; or
 - (c) an ancillary offence relating to an offence of a kind referred to in paragraph (a) or (b) of this subsection;has been committed, the succeeding provisions of this section have effect, whether or not the interception contravened subsection 7(1).

Section 72

- (2) The person may communicate the relevant information to:
- (a) the Attorney-General; or
 - (aa) the Minister; or
 - (b) the Director of Public Prosecutions; or
 - (c) the Commissioner of Police; or
 - (ca) the Integrity Commissioner; or
 - (d) the Chief Executive Officer of the ACC.
- (3) A person to whom the relevant information is communicated in accordance with subsection (2) may, for a purpose connected with:
- (a) an investigation of a suspected offence;
 - (b) the making by an authority, body or person of a decision whether or not to begin a proceeding by way of a prosecution for a suspected offence; or
 - (c) a proceeding by way of a prosecution for a suspected offence;
- or for 2 or more such purposes, and for no other purpose, communicate to another person, make use of, or make a record of, some or all of the relevant information.

72 Making record for purpose of permitted communication

A person who is permitted by section 63B, 63C, 63D, 63E, 65 or 65A, subsection 66(1), section 68 or subsection 71(2) to communicate particular information to another person may, for the purpose of so communicating the information in accordance with that section or subsection, make a record of the information, or cause such a record to be made.

73 Further dealing by recipient of certain information

- (1) Subject to subsections (2) and (3), a person to whom information has, in accordance with section 63A, subsection 63B(2), 63C(2) or 63D(2), section 67, subsection 71(3) or this subsection, been communicated for a purpose, or for 2 or more purposes, may, for that purpose, or for one or more of those purposes, and for no other

purpose, communicate to another person, make use of, or make a record of, that information.

- (2) If a person to whom information has been communicated in accordance with subsection 63D(2) communicates the information to another person (the *recipient*) under subsection (1) of this section, the recipient must not communicate, use, or make a record of, the information under subsection (1) of this section if the recipient would contravene another law of the Commonwealth, or a law of a State or Territory, in doing so.
- (3) If the recipient communicates that information to a third person under subsection (1) of this section, the third person must not communicate, use, or make a record of, the information under that subsection if the third person would contravene another law of the Commonwealth, or a law of a State or Territory, in doing so.

74 Giving information in evidence in exempt proceeding

- (1) A person may give lawfully intercepted information (other than foreign intelligence information, general computer access intercept information, data disruption intercept information, network activity warrant intercept information or ASIO computer access intercept information) in evidence in an exempt proceeding.
- (2) For the purposes of applying subsection (1) in relation to information, the question whether or not a communication was intercepted in contravention of subsection 7(1) may be determined on the balance of probabilities.
- (3) A person may give interception warrant information in evidence in an exempt proceeding.

75 Giving information in evidence where defect in connection with warrant

- (1) Where a communication has been intercepted in contravention of subsection 7(1) but purportedly under a warrant (other than a general computer access warrant, a data disruption warrant, a

Section 75A

network activity warrant or a warrant under section 11A, 11B or 11C), a person may give information obtained by the interception in evidence in an exempt proceeding, being a proceeding in a court or before a tribunal, body, authority or person, if the court, tribunal, body, authority or person, as the case may be, is satisfied that:

- (a) but for an irregularity, the interception would not have constituted a contravention of subsection 7(1); and
 - (b) in all the circumstances, the irregularity should be disregarded.
- (2) A reference in subsection (1) to an irregularity is a reference to a defect or irregularity (other than a substantial defect or irregularity):
- (a) in, or in connection with the issue of, a document purporting to be a warrant; or
 - (b) in connection with the execution of a warrant, or the purported execution of a document purporting to be a warrant.

75A Evidence that has been given in exempt proceeding

If information is given in evidence (whether before or after the commencement of this section) in an exempt proceeding under section 74 or 75, that information, or any part of that information, may later be given in evidence in any proceeding.

Note: This section was inserted as a response to the decision of the Court of Appeal of New South Wales in *Wood v Beves* (1997) 92 A Crim R 209.

76 Giving information in evidence in criminal proceedings under this Act

- (1) A person may give information obtained by intercepting a communication in contravention of subsection 7(1) in evidence in a proceeding by way of a prosecution for:
 - (a) an offence against subsection 7(1) constituted by the interception, or by authorising, suffering or permitting, or doing any act or thing to enable, the interception;

- (b) an offence against section 63 constituted by communicating to a person, making use of, making a record of, or giving in evidence in a proceeding, information obtained by the interception; or
 - (c) an ancillary offence relating to an offence of a kind referred to in paragraph (a) or (b) of this subsection.
- (2) A person may give interception warrant information in evidence in a proceeding by way of a prosecution for:
- (a) an offence against subsection 7(1); or
 - (b) an offence against section 63; or
 - (c) an ancillary offence relating to an offence of a kind referred to in paragraph (a) or (b) of this subsection.

76A Giving information in evidence in civil proceedings for remedial relief

- (1) A person may give information obtained by intercepting a communication in contravention of subsection 7(1) in evidence in a proceeding by way of an application under section 107A for remedial relief in respect of:
- (a) the interception; or
 - (b) the communication (in contravention of section 63) of information obtained by the interception.
- (2) A person may give interception warrant information in evidence in a proceeding by way of an application under section 107A.

77 Intercepted material and interception warrant information inadmissible except as provided

- (1) Where a communication passing over a telecommunications system has been intercepted, whether or not in contravention of subsection 7(1), then:
- (a) subject to paragraph (b), neither information, nor a record, obtained by the interception is admissible in evidence in a proceeding except in so far as section 63A, 63AB, 63AC,

Section 78

- 63AD, 63AE, 74, 75, 75A, 76 or 76A permits a person to give in evidence in that proceeding information so obtained; and
- (b) for the purpose of determining the extent (if any) to which section 63A, 63AB, 63AC, 63AD, 63AE, 74, 75, 75A, 76 or 76A permits a person to give in evidence in a proceeding information obtained by the interception:
- (i) a person may communicate to another person, make use of, make a record of, or give in evidence in the last-mentioned proceeding, information so obtained; and
 - (ii) information, or a record, so obtained is admissible in evidence in the last-mentioned proceeding.
- (2) Neither information, nor a record, obtained by virtue of a warrant under section 11A, 11B or 11C is admissible in evidence in a proceeding unless section 63A, 74 or 75A permits a person to give in evidence in that proceeding information obtained by virtue of the warrant.
- (3) Interception warrant information is admissible in evidence in a proceeding only to the extent that section 63AA, 74, 75A, 76 or 76A permits a person to give interception warrant information in evidence in that proceeding.
- (4) For the purpose of determining the extent (if any) to which section 63AA, 74, 75A, 76 or 76A permits a person to give interception warrant information in evidence in a proceeding:
- (a) a person may:
 - (i) communicate the information to another person; or
 - (ii) make use of the information; or
 - (iii) make a record of the information; or
 - (iv) give the information in evidence in the proceeding; and
 - (b) the information is admissible in evidence in the proceeding.

78 Where evidence otherwise inadmissible

Nothing in this Part renders information, or a restricted record, admissible in evidence in a proceeding to a greater extent than it

would have been admissible in evidence in that proceeding if this Part had not been enacted.

79 Destruction of restricted records that are not likely to be required for a permitted purpose

- (1) Where:
 - (a) a restricted record (whether made before or after the commencement of this section) is in the possession of an agency (other than an eligible authority of a State in relation to which a declaration is in force under section 34); and
 - (b) the chief officer of the agency is satisfied that the restricted record is not likely to be required for a permitted purpose in relation to the agency;the chief officer shall cause the restricted record to be destroyed forthwith.
- (2) In spite of subsection (1), a restricted record must not be destroyed unless the agency has received from the Secretary of the Department written notice that the entry in the General Register relating to the warrant under which the record was obtained has been inspected by the Minister.
- (3) This section does not apply to a restricted record that is a record of a communication that was intercepted under paragraph 7(2)(aaa).

79AA Destruction of restricted records—information obtained before a Part 5.3 supervisory order came into force

- (1) If:
 - (a) a restricted record is in the possession of an agency; and
 - (b) the restricted record relates to an interception authorised by a Part 5.3 supervisory order warrant; and
 - (c) the warrant was issued for the purpose, or for purposes that include the purpose, of obtaining information that would be likely to assist in connection with determining whether the relevant Part 5.3 supervisory order, or any succeeding

Section 79A

Part 5.3 supervisory order, has been, or is being, complied with; and

- (d) the interception occurred when the Part 5.3 supervisory order had been made but had not come into force; and
- (e) the chief officer of the agency is satisfied that none of the information obtained by the interception is likely to assist in connection with achieving a Part 5.3 object;

the chief officer of the agency must cause the restricted record to be destroyed as soon as practicable.

- (2) Section 6T does not apply to subsection (1) of this section.

79A Responsible person for a computer network must ensure restricted records are destroyed

- (1) This section applies if:
 - (a) a restricted record is a record of a communication that was intercepted under paragraph 7(2)(aaa); and
 - (b) the restricted record is in the possession of:
 - (i) a responsible person for the computer network concerned; or
 - (ii) the individual or body (whether or not a body corporate) who operates the network, or on whose behalf the network is operated; or
 - (iii) a person engaged in network protection duties in relation to the network.
- (2) The responsible person must cause the restricted record to be destroyed as soon as practicable after becoming satisfied that the restricted record is not likely to be required:
 - (a) for the purpose of enabling a person to perform the person's network protection duties in relation to the network; or
 - (b) if the network is operated by, or on behalf of, a Commonwealth agency, security authority or eligible authority of a State—for any of the following purposes:

Section 79A

- (i) determining whether disciplinary action should be taken in relation to a use of the network by an employee, office holder or contractor of the agency or authority;
- (ii) taking disciplinary action in relation to a use of the network by such an employee, office holder or contractor in a case where the use is not an appropriate use of the network by that employee, office holder or contractor;
- (iii) reviewing a decision to take such disciplinary action.

Section 80

Part 2-7—Keeping and inspection of interception records

80 Commonwealth agencies to keep documents connected with issue of warrants

The chief officer of a Commonwealth agency must cause to be kept in the agency's records:

- (a) each warrant issued to the agency; and
- (b) a copy of each notification under subsection 59A(2), being a notification given to the Secretary of the Department; and
- (c) each instrument revoking such a warrant; and
- (d) a copy of each certificate issued under subsection 61(4) by a certifying officer of the agency; and
- (e) each authorisation by the chief officer under subsection 66(2); and
- (f) a copy of each advice the chief officer gives to the Minister under subsection 103B(2) or paragraph 103B(4)(b); and
- (g) each notice the chief officer receives from the Minister under paragraph 103B(3)(a) or (5)(a).

81 Other records to be kept by Commonwealth agencies in connection with interceptions

- (1) The chief officer of a Commonwealth agency must cause:
 - (a) particulars of each telephone application for a Part 2-5 warrant made by the agency; and
 - (b) in relation to each application by the agency for a Part 2-5 warrant, a statement as to whether:
 - (i) the application was withdrawn or refused; or
 - (ii) a warrant was issued on the application; and
 - (c) in relation to each Part 2-5 warrant whose authority is exercised by the agency, particulars of:

- (i) the warrant; and
 - (ii) the day on which, and the time at which, each interception under the warrant began; and
 - (iii) the duration of each such interception; and
 - (iv) the name of the person who carried out each such interception; and
 - (v) in relation to a named person warrant—each service to or from which communications have been intercepted under the warrant; and
- (d) in relation to each restricted record (other than a restricted record that is a record of a communication that was intercepted under paragraph 7(2)(aaa)) that has at any time been in the agency's possession, particulars of:
- (i) if the restricted record is a record obtained by an interception under a warrant issued to the agency—that warrant; and
 - (ii) each occasion when the restricted record came (whether by its making or otherwise) to be in the agency's possession; and
 - (iii) each occasion (if any) when the restricted record ceased (whether by its destruction or otherwise) to be in the agency's possession; and
 - (iv) each other agency or other body (if any) from or to which, or other person (if any) from or to whom, the agency received or supplied the restricted record; and
- (e) particulars of each use made by the agency of lawfully intercepted information; and
- (f) particulars of each communication of lawfully intercepted information by an officer of the agency to a person or body other than such an officer; and
- (g) particulars of each occasion when, to the knowledge of an officer of the agency, lawfully intercepted information was given in evidence in a relevant proceeding in relation to the agency; and

Section 81AA

- (h) particulars of each reconsideration by the chief officer under paragraph 103B(4)(a) that does not result in the chief officer giving advice under paragraph 103B(4)(b);
to be recorded in writing or by means of a computer as soon as practicable after the happening of the events to which the particulars relate or the statement relates, as the case may be.
- (2) If a Part 2-5 warrant is a named person warrant, the particulars referred to in subparagraph (1)(c)(ii) must indicate the service in respect of which each interception occurred.
- (2A) If:
- (a) the Organisation is exercising the authority conferred by a Part 2-5 warrant issued to a Commonwealth agency; and
 - (b) the Commonwealth agency does not have the particulars referred to in subparagraph (1)(c)(ii), (iii) or (iv), or paragraph (1)(d);
- the Director-General of Security must:
- (c) cause those particulars to be recorded in accordance with subsections (1) and (2); and
 - (d) give the records produced to the chief officer of the Commonwealth agency to which the Part 2-5 warrant was issued.
- (3) The chief officer of a Commonwealth agency must cause to be kept in the agency's records each record that the chief officer has caused to be made, or is given, under this section.

81AA Organisation to record particulars in relation to eligible authorities of a State

- If:
- (a) the Organisation is exercising the authority conferred by a Part 2-5 warrant issued to an eligible authority of a State; and
 - (b) the eligible authority does not have the particulars referred to in subparagraph 81(1)(c)(ii), (iii) or (iv), or paragraph 81(1)(d);

the Director-General of Security must:

- (c) cause those particulars to be recorded in accordance with subsections 81(1) and (2); and
- (d) give the records produced to the chief officer of the eligible authority to which the Part 2-5 warrant was issued.

81A General Register of Warrants

- (1) The Secretary of the Department is to cause a General Register of Warrants to be kept.
- (2) The Secretary of the Department is to cause to be recorded in the General Register in relation to each Part 2-5 warrant particulars of:
 - (a) the date of issue of the warrant; and
 - (b) the Judge or nominated AAT member who issued the warrant; and
 - (c) the agency to which the warrant was issued; and
 - (d) in the case of a telecommunications service warrant:
 - (i) the telecommunications service to which the warrant relates; and
 - (ii) the name of the person specified in the warrant as a person using or likely to use the telecommunications service; and
 - (e) in the case of a named person warrant:
 - (i) the name of the person to whom the warrant relates; and
 - (ii) each telecommunications service that is specified in the warrant, or in relation to which interceptions authorised by the warrant have occurred; and
 - (f) the period for which the warrant is to be in force; and
 - (g) in the case of a warrant issued under subsection 46(1) or 46A(1), or issued under section 48 in the circumstances mentioned in subsection 46(1)—each serious offence in relation to which the Judge or nominated AAT member who issued the warrant was satisfied, on the application for the warrant, as mentioned in:

Section 81B

- (i) in the case of a warrant under section 48—
paragraph 46(1)(d); or
- (ii) otherwise—paragraph 46(1)(d) or 46A(1)(d), as the case
requires; and
- (h) in the case of a Part 5.3 warrant—the name of the person to
whom the relevant Part 5.3 supervisory order or application
relates.

81B Regular submission of General Register to Minister

- (1) Within 3 months after the commencement of Schedule 5 to the
Telecommunications (Interception) Amendment Act 2006, the
Secretary of the Department must deliver the General Register to
the Minister for inspection.
- (2) Once at least within each succeeding period of 3 months, the
Secretary of the Department must deliver to the Minister, for
inspection by the Minister, any part of the General Register that
represents information recorded since the General Register, or any
part of the General Register, was last delivered to the Minister.

81C Special Register of Warrants

Special Register of Warrants

- (1) The Secretary of the Department is to cause a ***Special Register of Warrants*** to be kept.

Contents of Register

- (2) The Secretary of the Department is to cause to be recorded in the
Special Register the following particulars in relation to each
registrable expired warrant:
 - (a) the date of issue of the warrant;
 - (b) the Judge or nominated AAT member who issued the
warrant;
 - (c) the agency to which the warrant was issued;
 - (d) in the case of a telecommunications service warrant:

Section 81C

- (i) the telecommunications service to which the warrant related; and
 - (ii) the name of the person specified in the warrant as a person using or likely to use the telecommunications service; and
- (e) in the case of a named person warrant:
- (i) the name of the person to whom the warrant related; and
 - (ii) each telecommunications service that is specified in the warrant, or in relation to which interceptions authorised by the warrant have occurred; and
- (f) the period for which the warrant was in force;
- (g) in the case of a warrant issued under subsection 46(1) or 46A(1), or issued under section 48 in the circumstances mentioned in subsection 46(1)—each serious offence in relation to which the Judge or nominated AAT member who issued the warrant was satisfied, on the application for the warrant, as mentioned in:
- (i) in the case of a warrant under section 48—paragraph 46(1)(d); or
 - (ii) otherwise—paragraph 46(1)(d) or 46A(1)(d), as the case requires;
- (h) in the case of a Part 5.3 warrant—the name of the person to whom the relevant Part 5.3 supervisory order or application relates.

Note: **Registrable expired warrant** is defined by subsections (3) and (4).

Registrable expired warrant—original warrant renewed

- (3) For the purposes of this section, if:
- (a) a Part 2-5 warrant has been issued; and
 - (b) the warrant was an original warrant; and
 - (c) there were one or more renewals of the warrant; and
 - (d) at the end of the period of 3 months after the time (the **cessation time**) when the last renewal of the warrant ceased to be in force, no criminal proceedings had been instituted, or were likely to be instituted, against a person on the basis of

Section 81C

information obtained as a result of intercepting a communication under:

- (i) the warrant; or
 - (ii) a renewal of the warrant; and
- (e) the cessation time is after the commencement of this section; the warrant, and each renewal of the warrant, becomes a **registrable expired warrant** at the end of that period.

Registrable expired warrant—original warrant not renewed

- (4) For the purposes of this section, if:
- (a) a Part 2-5 warrant has been issued; and
 - (b) the warrant was an original warrant; and
 - (c) no renewal of the warrant was issued; and
 - (d) at the end of the period of 3 months after the time (the **cessation time**) when the warrant ceased to be in force, no criminal proceedings had been instituted, or were likely to be instituted, against a person on the basis of information obtained as a result of intercepting a communication under the warrant; and
 - (e) the cessation time is after the commencement of this section; the warrant becomes a **registrable expired warrant** at the end of that period.

Interpretation—criminal proceedings supported by intercepted information

- (5) A reference in this section to criminal proceedings that had been, or were likely to be, instituted on the basis of information obtained as a result of intercepting a communication under a warrant includes a reference to criminal proceedings that were, or were likely to be, supported by information obtained as a result of intercepting a communication under a warrant.

81D Regular submission of Special Register to Minister

Original submission

- (1) Within 3 months after the commencement of Schedule 5 to the *Telecommunications (Interception) Amendment Act 2006*, the Secretary of the Department must deliver the Special Register to the Minister for inspection by the Minister.

Subsequent submissions

- (2) Once at least within each succeeding period of 3 months, the Secretary of the Department must deliver to the Minister, for inspection by the Minister, any part of the Special Register that represents information recorded since the Special Register, or any part of the Special Register, was last delivered to the Minister.

Special Register and General Register to be delivered at the same time

- (3) As far as is practicable, the Secretary of the Department is to ensure that delivery of the Special Register, or a part of the Special Register, as the case requires, takes place at the same time as the delivery of a part of the General Register under subsection 81B(2).

81E Provision of information by eligible authorities

When section applies

- (1) This section applies to an eligible authority of a State if the eligible authority is an agency.

Secretary may require information

- (2) The Secretary of the Department may, by written notice given to the chief officer of the eligible authority, require the chief officer to give the Secretary such information as the Secretary requires for the purposes of complying with the obligations imposed on him or her by section 81C.

Section 83

Information to be given

- (3) The chief officer must give the information within the period, and in the manner, specified in the notice.

83 Inspections

- (1) The Ombudsman shall inspect the records of each Commonwealth agency:
- (a) at least twice during the period beginning at the commencement of this Part and ending on 30 June 1988; and
 - (b) at least twice during each financial year beginning on or after 1 July 1988;
- in order to ascertain the extent to which the agency's officers have complied with sections 79, 79AA, 80 and 81 since that commencement, or since the last inspection under this Part of the agency's records, as the case requires.
- (2) The Ombudsman may at any time inspect a Commonwealth agency's records in order to ascertain the extent to which the agency's officers have complied during any period with sections 79, 79AA, 80 and 81.
- (3) The Ombudsman may inspect a Commonwealth agency's records in order to ascertain the extent to which officers of the agency have complied during any period with the conditions, restrictions and provisions mentioned in subsection 59B(2) (about Part 5.3 warrants) if:
- (a) the chief officer of the agency notifies the Ombudsman under that subsection of a contravention of any of those conditions, restrictions or provisions; and
 - (b) the contravention occurred in that period.
- (4) If:
- (a) the performance of a function, or the exercise of a power, conferred by Part 15 of the *Telecommunications Act 1997* is in connection with an interception warrant; and

(b) a Commonwealth agency has records that relate to the performance of that function or the exercise of that power; the Ombudsman may inspect those records in order to ascertain the extent to which the agency's officers have complied with Part 15 of the *Telecommunications Act 1997*.

84 Reports

- (1) The Ombudsman shall, as soon as practicable, and in any event within 3 months, after the end of each financial year, report to the Minister in writing, in relation to each Commonwealth agency, about the results of the inspections under subsections 83(1), (3) and (4), during that financial year, of the agency's records.
 - (1A) The Ombudsman must include in each report under subsection (1) in relation to a financial year:
 - (a) a summary of the inspections conducted in the financial year under section 83; and
 - (b) particulars of any deficiencies identified that impact on the integrity of the telecommunications interception regime established by this Act; and
 - (c) particulars of the remedial action (if any) taken or proposed to be taken to address those deficiencies.
- Note: In complying with this section, the Ombudsman remains bound by the obligations imposed by section 63 relating to disclosure of intercepted information or interception warrant information.
- (2) The Ombudsman may report to the Minister in writing at any time about the results of an inspection under this Part and shall do so if so requested by the Minister.
 - (3) The Ombudsman shall give a copy of a report under subsection (1) or (2) to the chief officer of the agency to which the report relates.

85 Ombudsman may report on other breaches of this Act

- (1) If, as a result of an inspection under this Part of the records of an agency, the Ombudsman is of the opinion that an officer of the

Section 85A

agency has contravened a provision of this Act, the Ombudsman may include in his or her report on the inspection a report on the contravention.

- (2) To avoid doubt, for the purposes of subsection (1), a contravention of a condition or restriction specified in a warrant issued under this Act is a contravention of a provision of this Act.
- (3) Subsection (1) does not apply to a contravention of section 79, 79AA, 80 or 81.

85A Annual report may cover notified breaches in relation to Part 5.3 warrants

- (1) In a report under subsection 84(1) in relation to a financial year, the Ombudsman may include a report on a contravention of which the Ombudsman is notified under subsection 59B(2) (about Part 5.3 warrants), if the Ombudsman does not conduct an inspection under subsection 83(3) in relation to a period during which the contravention occurred.

Note: If the Ombudsman conducts an inspection under subsection 83(3), the relevant report under subsection 84(1):

- (a) must include the matters mentioned in subsection 84(1A) in relation to the inspection; and
 - (b) may include other information about contraventions of this Act (see section 85).
- (2) For the purposes of subsection (1), it does not matter whether the Ombudsman is notified under subsection 59B(2) before, during or after the financial year to which the report relates.
 - (3) Subsection (1) does not limit what the Ombudsman may include in a report under section 84 or 85.

86 Ombudsman's general powers

- (1) For the purposes of an inspection under this Part of an agency's records, the Ombudsman:
 - (a) may, after notifying the chief officer of the agency, enter at any reasonable time premises occupied by the agency; and
-

- (b) is entitled to have full and free access at all reasonable times to all records of the agency; and
 - (ba) is entitled to have full and free access at all reasonable times to the General Register and the Special Register; and
 - (c) notwithstanding section 63 or any other law, is entitled to make copies of, and to take extracts from, records of the agency or the General Register or Special Register; and
 - (d) may require an officer of the agency to give the Ombudsman such information as the Ombudsman considers necessary, being information that is in the officer's possession, or to which the officer has access, and that is relevant to the inspection.
- (2) The chief officer of a Commonwealth agency shall ensure that the agency's officers provide to the Ombudsman such assistance in connection with the performance or exercise of the Ombudsman's functions or powers under this Part as the Ombudsman reasonably requires.
- (3) The Ombudsman's powers include doing anything incidental or conducive to the performance of any of the Ombudsman's functions under this Part.

87 Power to obtain relevant information

- (1) Where the Ombudsman has reason to believe that an officer of an agency is able to give information relevant to an inspection under this Part of the agency's records, subsections (2) and (3) have effect.
- (2) The Ombudsman may, by writing given to the officer, require the officer to give the information to the Ombudsman:
- (a) by writing signed by the officer; and
 - (b) at a specified place and within a specified period.
- (3) The Ombudsman may, by writing given to the officer, require the officer to attend:
- (a) before a specified inspecting officer;

Section 88

- (b) at a specified place; and
 - (c) within a specified period or at a specified time on a specified day;
- in order to answer questions relevant to the inspection.
- (4) Where the Ombudsman:
- (a) has reason to believe that an officer of an agency is able to give information relevant to an inspection under this Part of the agency's records; and
 - (b) does not know the officer's identity;
- the Ombudsman may, by writing given to the chief officer of the agency, require the chief officer, or a person nominated by the chief officer, to attend:
- (c) before a specified inspecting officer;
 - (d) at a specified place; and
 - (e) within a specified period or at a specified time on a specified day;
- in order to answer questions relevant to the inspection.
- (5) The place, and the period or the time and day, specified in a requirement under this section shall be reasonable having regard to the circumstances in which the requirement is made.
- (6) A person must not refuse:
- (a) to attend before a person; or
 - (b) to give information; or
 - (c) to answer questions;
- when required to do so under this section.

Penalty for an offence against this subsection: Imprisonment
for 6 months.

88 Ombudsman to be given information and access notwithstanding other laws

- (1) Notwithstanding any other law, a person is not excused from giving information, answering a question, or giving access to a

document, as and when required by or under this Part, on the ground that giving the information, answering the question, or giving access to the document, as the case may be, would contravene a law, would be contrary to the public interest or might tend to incriminate the person or make the person liable to a penalty, but:

- (a) the information, the answer, or the fact that the person has given access to the document, as the case may be; and
- (b) any information or thing (including a document) obtained as a direct or indirect consequence of giving the first-mentioned information, answering the question or giving access to the first-mentioned document, as the case may be;

is not admissible in evidence against the person except in a proceeding by way of a prosecution for an offence against section 107.

- (2) Nothing in section 63 or any other law prevents an officer of an agency from:
 - (a) giving information to an inspecting officer (whether orally or in writing and whether or not in answer to a question); or
 - (b) giving to an inspecting officer access to a record of the agency;for the purposes of an inspection under this Part of the agency's records.
- (3) Nothing in section 63 or any other law prevents an officer of an agency from making a record of information, or causing a record of information to be made, for the purposes of giving the information to a person as permitted by subsection (2).

89 Dealing with information for the purposes of inspection and report

Where:

- (a) information is given or communicated to an inspecting officer, as permitted by subsection 88(2) or this section, for

Section 90

the purposes of an inspection, or of a report on an inspection, under this Part of an agency's records; or

- (b) an inspecting officer obtains information as a result of being given access to records of an agency, as permitted by subsection 88(2), for the purposes of an inspection under this Part of the agency's records;

the inspecting officer may, notwithstanding section 63 or any other law, communicate to another inspecting officer, make use of, or make a record of, the information for the purposes of an inspection, or of a report on an inspection, under this Part of the agency's records.

90 Ombudsman not to be sued

Subject to the provisions applying by virtue of subsection 92(3), an inspecting officer, or a person acting under an inspecting officer's direction or authority, is not liable to an action, suit or proceeding for or in relation to an act done, or omitted to be done, in good faith in the performance or exercise, or the purported performance or exercise, of a function, power or authority conferred by this Part.

91 Delegation by Ombudsman

- (1) The Ombudsman may, either generally or as otherwise provided by the instrument of delegation, delegate to another inspecting officer, all or any of the Ombudsman's powers under this Part other than a power to report to the Minister and this power of delegation.
- (2) A power so delegated, when exercised by the delegate, shall, for the purposes of this Part, be deemed to have been exercised by the Ombudsman.
- (3) A delegation under subsection (1) does not prevent the exercise of a power by the Ombudsman.
- (4) A delegate shall, upon request by a person affected by the exercise of any power delegated to the delegate, produce the instrument of delegation, or a copy of the instrument, for inspection by the person.

92 Application of Ombudsman Act

- (1) Section 11A of the *Ombudsman Act 1976* does not apply in relation to the exercise or proposed exercise of a power, or the performance or the proposed performance of a function, of the Ombudsman under this Part.
- (2) A reference in section 19 of the *Ombudsman Act 1976* to the Ombudsman's operations does not include a reference to anything that an inspecting officer has done or omitted to do under this Part.
- (3) Subject to section 88 of this Act, subsections 35(2), (3), (4) and (8) of the *Ombudsman Act 1976* apply for the purposes of this Part and so apply as if:
 - (a) a reference in those subsections to an officer were a reference to an inspecting officer;
 - (b) a reference in those subsections to information did not include a reference to lawfully intercepted information;
 - (c) a reference in those subsections to that Act were a reference to this Part;
 - (d) paragraph 35(3)(b) of that Act were omitted; and
 - (e) section 35A of that Act had not been enacted.

92A Exchange of information between Ombudsman and State inspecting authorities

- (1) In this section:

State agency means an eligible authority of a State that is an agency.

State inspecting authority, in relation to a State agency, means the authority that, under the law of the State concerned, has the function of making inspections of the kind referred to in paragraph 35(1)(h).

- (2) The Ombudsman may give information that:
 - (a) relates to a State agency; and
 - (b) was obtained by the Ombudsman under this Act;

Section 92A

to the authority that is the State inspecting authority in relation to the agency.

- (3) The Ombudsman may only give information to an authority under subsection (2) if the Ombudsman is satisfied that the giving of the information is necessary to enable the authority to perform its functions in relation to the State agency.
- (4) The Ombudsman may receive from a State inspecting authority information relevant to the performance of the Ombudsman's functions under this Act.

Part 2-8—Reports about interceptions under Parts 2-3 and 2-5

Division 1—Reports to the Minister

93 Annual reports to Minister about interceptions under Part 2-3

The Managing Director of a carrier shall, as soon as practicable after each 30 June, give to the Minister a written report about the interceptions carried out by employees of the carrier pursuant to requests made, or purporting to be made, under section 30 during the year ending on that 30 June.

94 Annual reports regarding applications and warrants under Part 2-5

- (2) The chief officer of a Commonwealth agency must give to the Minister, within 3 months after a telecommunications service warrant issued to the agency ceases to be in force, a written report containing:
 - (a) information about:
 - (i) the use made by the agency of information obtained by interceptions under the warrant; and
 - (ii) the communication of such information to persons other than officers of the agency; and
 - (iii) the number of arrests that have been, or are likely to be, made on the basis of such information; and
 - (b) an assessment of the usefulness of information obtained by interceptions under the warrant.
- (3) The chief officer of a Commonwealth agency shall, as soon as practicable, and in any event within 3 months, after each 30 June, give to the Minister a written report that sets out such information as:

Section 94A

- (a) Division 2 (other than section 102B) requires to be set out in the Minister's report under that Division relating to the year ending on that 30 June; and
 - (b) can be derived from the agency's records.
- (3A) A report under subsection (3) must include a statement of the total expenditure (including expenditure of a capital nature) incurred by the agency concerned in connection with the execution of warrants during the year to which the report relates.
- (4) Section 34C of the *Acts Interpretation Act 1901* does not apply in relation to a report under subsection (3) of this section.

94A Reports regarding emergency interception action

- (1) The chief officer of an agency referred to in subsection 7(8) must give to the Minister a written report concerning:
- (a) an emergency interception action taken by an officer of the agency that, because of the operation of subsection 7(6A), took place without a warrant under Part 2-5; and
 - (b) an emergency interception action taken by an officer of the agency in respect of which an application for a warrant was made under Part 2-5 and refused.
- (2) The chief officer of the agency must give the report within 3 months after:
- (a) in the case set out in paragraph (1)(a)—the date on which the action ceased; and
 - (b) in the case set out in paragraph (1)(b)—the date on which the application was refused.
- (3) The report must contain the following information:
- (a) if an interception occurred:
 - (i) the date and time at which the interception began; and
 - (ii) the duration of the interception;
 - (b) if there was no interception but action had been taken to cause a communication to be intercepted—details of the action taken;

- (c) the circumstances that led the officer concerned to believe that the conditions of subsection 7(4) or (5) were satisfied;
 - (d) in the case set out in paragraph (1)(a)—the reasons it was not practicable to apply for a warrant under Part 2-5 in relation to the action;
 - (e) in the case set out in paragraph (1)(b)—the reasons the judge or nominated AAT member refused the application if the reasons are known;
 - (f) information about the use made by the agency of information obtained by the interception;
 - (g) information about the communication of such information to persons other than officers of the agency;
 - (h) the number of arrests that have been, or are likely to be, made on the basis of such information;
 - (i) an assessment of the usefulness of information obtained by the interception.
- (4) In this section:

emergency interception action means an interception done under subsection 7(4) or (5) or action taken under one of those subsections to cause an interception to occur.

94B Reports regarding named person warrants

- (1) The chief officer of an agency to which a named person warrant has been issued must give to the Minister a written report about the action (if any) that has taken place under the warrant.
- (2) The chief officer must give a report in relation to the warrant within 3 months after the warrant ceases to be in force.
- (3) The report must contain the following information in relation to each interception:
 - (a) the service to or from which the intercepted communication was made (being a service that the person named in the warrant used, or was likely to use);

Section 95

- (b) the reasons it would not have been effective to intercept the communications under a telecommunications service warrant;
- (c) information about the use made by the agency of information obtained by each interception;
- (d) information about the communication of such information to persons other than officers of the agency;
- (e) the number of arrests that have been, or are likely to be, made on the basis of such information;
- (f) an assessment of the usefulness of information obtained by each interception.

95 Minister may seek further information from Commonwealth agency

- (1) The Minister may by writing request the chief officer of a Commonwealth agency, or eligible Commonwealth authority, to give to the Minister in writing specified information that:
 - (a) the Minister needs in connection with preparing a report under Division 2; and
 - (b) is not contained in a report by the chief officer under subsection 94(3).
- (2) To the extent that it is practicable to do so, the chief officer of a Commonwealth agency, or eligible Commonwealth authority, shall comply with a request made to the chief officer under subsection (1).

96 Annual reports by State authorities

- (1) Subject to subsection (2), the chief officer of an eligible authority of a State shall, as soon as practicable, and in any event within 3 months, after each 30 June, give to the Minister a written report that:
 - (a) if information that section 102 or 102A requires to be set out in the Minister's report under Division 2 relating to the year

ending on that 30 June can be derived from the authority's records—sets out that information; or

(b) in any other case—states that no such information can be so derived.

(1A) A report under subsection (1) must include a statement of the total expenditure (including expenditure of a capital nature) incurred by the eligible authority concerned in connection with the execution of warrants during the year to which the report relates.

(2) Where a Minister of a State has given to the Minister a written report that sets out the information that, but for this subsection, subsections (1) and (1A) would require to be set out in a report by the chief officer of an eligible authority of that State, the chief officer need not give to the Minister the last-mentioned report.

97 Reports by Managing Directors about acts done in connection with certain warrants under Part 2-5

The Managing Director of a carrier shall give to the Minister, within 3 months after a warrant under section 46 or 46A ceases to be in force, a written report about the acts or things done by or in relation to employees of the carrier:

(a) to enable, or in connection with enabling, communications to be intercepted under the warrant; and

(b) to ensure discontinuance of interceptions under the warrant; and the days on which, and the times at which, those acts or things were done.

Division 2—Reports by the Minister

99 Annual report by Minister about warrants under Part 2-5

The Minister shall, as soon as practicable after each 30 June, cause to be prepared a written report that relates to the year ending on that 30 June and complies with this Division.

100 Report to set out how many applications made and warrants issued

- (1) The report shall set out, for each Commonwealth agency, and for each eligible authority of a State that was an agency at any time during that year:
 - (a) the relevant statistics about applications for Part 2-5 warrants that the agency or authority made during that year; and
 - (b) the relevant statistics about telephone applications for Part 2-5 warrants that the agency or authority made during that year; and
 - (c) the relevant statistics about renewal applications that the agency or authority made during that year; and
 - (d) the relevant statistics about applications for Part 2-5 warrants that the agency or authority made during that year and that included requests that the warrants authorise entry on premises; and
 - (e) how many Part 2-5 warrants issued on applications made by the agency or authority during that year specified conditions or restrictions relating to interceptions under the warrants; and
 - (ea) in relation to the applications of a kind referred to in paragraph (a), (b), (c) or (e), the relevant statistics about applications of that kind that relate to named person warrants; and
 - (eb) in relation to all named person warrants issued during that year on application made by each agency or authority:

- (i) how many of those warrants involved the interception of a single telecommunications service; and
 - (ii) how many of those warrants involved the interception of between 2 and 5 telecommunications services; and
 - (iii) how many of those warrants involved the interception of between 6 and 10 telecommunications services; and
 - (iv) how many of those warrants involved the interception of more than 10 telecommunications services; and
- (ec) in relation to all named person warrants issued during that year on application made by each agency or authority:
- (i) the total number of telecommunications services intercepted under those of the warrants that did not authorise the interception of communications made by means of a telecommunications device or telecommunications devices identified in the warrant; and
 - (ii) the total number of telecommunications services intercepted under those of the warrants that did authorise the interception of communications made by means of a telecommunications device or telecommunications devices identified in the warrant; and
 - (iii) the total number of telecommunications devices by means of which communications were intercepted under those of the warrants that did authorise the interception of communications made by means of a telecommunications device or telecommunications devices identified in the warrant; and
- (ed) in relation to applications of a kind referred to in paragraph (a), (b), (c), (d) or (e), the relevant statistics about applications of that kind that relate to warrants in relation to which subparagraph 46(1)(d)(ii) would apply if the warrants were issued; and
- (f) the categories of the serious offences specified under subsection 49(7) in Part 2-5 warrants issued on applications made by the agency or authority during that year; and

Section 100

(g) in relation to each of those categories, how many serious offences in that category were so specified.

(2) The report shall set out:

- (a) the relevant statistics about applications for Part 2-5 warrants that were made during that year; and
- (b) the relevant statistics about telephone applications for Part 2-5 warrants that were made during that year; and
- (c) the relevant statistics about renewal applications made during that year; and
- (d) the relevant statistics about applications for Part 2-5 warrants that were made during that year and that included requests that the warrants authorise entry on premises; and
- (e) how many Part 2-5 warrants issued on applications made during that year specified conditions or restrictions relating to interceptions under the warrants; and
- (ea) in relation to the applications of a kind referred to in paragraph (a), (b), (c) or (e), the relevant statistics about applications of that kind that relate to named person warrants; and
- (eb) in relation to all named person warrants issued during that year:
 - (i) how many of those warrants involved the interception of a single telecommunications service; and
 - (ii) how many of those warrants involved the interception of between 2 and 5 telecommunications services; and
 - (iii) how many of those warrants involved the interception of between 6 and 10 telecommunications services; and
 - (iv) how many of those warrants involved the interception of more than 10 telecommunications services; and
- (ec) in relation to all named person warrants issued during that year:
 - (i) the total number of telecommunications services intercepted under those of the warrants that did not authorise the interception of communications made by means of a telecommunications device or

- telecommunications devices identified in the warrant;
and
- (ii) the total number of telecommunications services intercepted under those of the warrants that did authorise the interception of communications made by means of a telecommunications device or telecommunications devices identified in the warrant;
and
 - (iii) the total number of telecommunications devices by means of which communications were intercepted under those of the warrants that did authorise the interception of communications made by means of a telecommunications device or telecommunications devices identified in the warrant; and
- (ed) in relation to applications of a kind referred to in paragraph (a), (b), (c), (d) or (e), the relevant statistics about applications of that kind that relate to warrants in relation to which subparagraph 46(1)(d)(ii) would apply if the warrants were issued; and
- (f) the categories of the serious offences specified under subsection 49(7) in Part 2-5 warrants issued on applications made during that year; and
- (g) in relation to each of those categories, how many serious offences in that category were so specified.

101 Report to contain particulars about duration of warrants

- (1) The report shall set out, for each Commonwealth agency, and for each eligible authority of a State that was an agency at any time during that year:
- (a) the average of the respective periods specified, in the Part 2-5 warrants that are original warrants and were issued on applications made by the agency or authority during that year, as the periods for which the warrants were to be in force; and
 - (b) the average of the respective periods during which the warrants referred to in paragraph (a) were in force; and

Section 101

- (c) the average of the respective periods specified, in the Part 2-5 warrants that are renewals of other warrants and were issued on applications made by the agency or authority during that year, as the periods for which the renewals were to remain in force; and
 - (d) the average of the respective periods during which the warrants first referred to in paragraph (c) were in force; and
 - (da) in relation to periods of a kind referred to in paragraph (a), (b), (c) or (d), the averages of the periods of that kind that relate to warrants in relation to which subparagraph 46(1)(d)(ii) applied; and
 - (e) how many 90 day final renewals, how many 150 day final renewals, and how many 180 day final renewals, being warrants issued to the agency or authority, ceased during that year to be in force.
- (2) The report shall set out:
- (a) the average of the respective periods specified, in Part 2-5 warrants that are original warrants and were issued on applications made during the year, as the periods for which the warrants were to be in force; and
 - (b) the average of the respective periods during which the warrants referred to in paragraph (a) were in force; and
 - (c) the average of the respective periods specified, in the Part 2-5 warrants that are renewals of other warrants and were issued on applications made during that year, as the periods for which the renewals were to remain in force; and
 - (d) the average of the respective periods during which the warrants first referred to in paragraph (c) were in force; and
 - (da) in relation to periods of a kind referred to in paragraph (a), (b), (c) or (d), the averages of the periods of that kind that relate to warrants in relation to which subparagraph 46(1)(d)(ii) applied; and
 - (e) how many 90 day final renewals, how many 150 day final renewals, and how many 180 day final renewals, ceased during that year to be in force.

- (3) A reference in subsection (1) or (2) to a 90 day final renewal, to a 150 day final renewal or to a 180 day final renewal is a reference to a warrant:
- (a) that is the last renewal of an original warrant; and
 - (b) that ceased to be in force:
 - (i) more than 90 days but not more than 150 days;
 - (ii) more than 150 days but not more than 180 days; or
 - (iii) more than 180 days;as the case may be, after the day of issue of that original warrant.

102 Report to contain information about effectiveness of warrants

- (1) The report shall set out, for each Commonwealth agency, for each eligible Commonwealth authority, and for each eligible authority of a State:
- (a) how many arrests were made during that year:
 - (i) in connection with the performance by the agency or authority of its functions; and
 - (ii) on the basis of information that was or included lawfully intercepted information;
 - (b) the categories of the prescribed offences proceedings by way of prosecutions for which ended during that year, being proceedings in which, according to the records of the agency or authority, lawfully intercepted information was given in evidence; and
 - (c) in relation to each of those categories:
 - (i) the number of such offences in that category; and
 - (ii) the number of such offences in that category in respect of which convictions were recorded.
- (2) The report shall set out:
- (a) how many arrests were made during that year:
 - (i) in connection with the performance by Commonwealth agencies, by eligible Commonwealth authorities, and by

Section 102

- eligible authorities of States, of their respective functions; and
- (ii) on the basis of information that was or included lawfully intercepted information;
- (b) the categories of the prescribed offences proceedings by way of prosecutions for which ended during that year, being proceedings in which, according to the respective records of Commonwealth agencies, of eligible Commonwealth authorities, and of eligible authorities of States, lawfully intercepted information was given in evidence; and
- (c) in relation to each of those categories:
- (i) the number of such offences in that category; and
 - (ii) the number of such offences in that category in respect of which convictions were recorded.
- (3) The report is to set out, for:
- (a) each Commonwealth agency; and
 - (b) each eligible authority of a State, where the eligible authority was an agency at any time during the year to which the report relates;

the percentage worked out using the formula:

$$\frac{\text{Eligible warrants}}{\text{Total warrants}} \times 100$$

where:

Eligible warrants means the number of warrants that satisfy the following conditions:

- (a) the warrant was issued to the agency or authority, as the case requires;
- (b) the warrant was in force during the year to which the report relates;
- (c) a prosecution was instituted, or was likely to be instituted, on the basis of information obtained by interceptions under:
 - (i) the warrant; or

- (ii) if the warrant was a renewal of an original warrant:
 - (A) the original warrant; or
 - (B) any other renewal of the original warrant; or
- (iii) if the warrant was an original warrant—any renewal of the original warrant.

Total warrants means the number of warrants that were:

- (a) issued to the agency or authority, as the case requires; and
 - (b) in force during the year to which the report relates.
- (4) The report is to set out the percentage worked out using the formula:

$$\frac{\text{Eligible warrants}}{\text{Total warrants}} \times 100$$

where:

Eligible warrants means the number of warrants that satisfy the following conditions:

- (a) the warrant was issued to:
 - (i) a Commonwealth agency; or
 - (ii) an eligible authority of a State, where the eligible authority was an agency at any time during the year to which the report relates;
- (b) the warrant was in force during the year to which the report relates;
- (c) a prosecution was instituted, or was likely to be instituted, on the basis of information obtained by interceptions under:
 - (i) the warrant; or
 - (ii) if the warrant was a renewal of an original warrant:
 - (A) the original warrant; or
 - (B) any other renewal of the original warrant; or
 - (iii) if the warrant was an original warrant—any renewal of the original warrant.

Section 102A

Total warrants means the number of warrants that were:

- (a) issued to:
 - (i) Commonwealth agencies; and
 - (ii) eligible authorities of States, where the eligible authorities were agencies at any time during the year to which the report relates; and
 - (b) in force during the year to which the report relates.
- (5) A reference in this section to a prosecution that was instituted, or was likely to be instituted, on the basis of information obtained by interceptions under a warrant includes a reference to a prosecution that was supported, or likely to be supported, by information obtained by interceptions under a warrant.

102A Report regarding interceptions without warrant

The report must state, for each agency referred to in subsection 7(8), the number of occasions on which an officer or staff member of the agency intercepted a communication in reliance on subsection 7(4) or (5).

102B Report regarding international requests

The report must set out the number of occasions on which lawfully intercepted information or interception warrant information was communicated to any of the following:

- (a) a foreign country under paragraph 68(l) or section 68A;
- (b) the International Criminal Court under paragraph 68(la) or section 68A;
- (c) a War Crimes Tribunal under paragraph 68(lb) or section 68A.

103 Other information to be included in report

The report must set out:

- (a) the total expenditure (including expenditure of a capital nature) incurred by agencies to which the report relates in

connection with the execution of warrants during the year to which the report relates; and

- (aa) for:
- (i) each Commonwealth agency; and
 - (ii) each eligible authority of a State, where the eligible authority was an agency at any time during the year to which the report relates;

the amount worked out using the formula:

$$\frac{\text{Total warrant expenditure}}{\text{Number of warrants}}$$

where:

Total warrant expenditure means the total expenditure (including expenditure of a capital nature) incurred by the agency or the authority, as the case requires, in connection with the execution of warrants during the year to which the report relates.

Number of warrants means the number of warrants to which the total warrant expenditure relates; and

- (ab) information about the availability of judges to issue warrants under Part 2-5 and the extent to which nominated AAT members have been used for that purpose, but not including information that would identify a particular judge or AAT member; and

- (ac) for:
- (i) each Commonwealth agency; and
 - (ii) each eligible authority of a State, where the eligible authority was an agency at any time during the year to which the report relates;

the number (if any) of interceptions carried out on behalf of each other such Commonwealth agency or eligible authority; and

- (aca) the number (if any) of interceptions carried out by the Organisation on behalf of:
- (i) each Commonwealth agency; and

Section 103A

- (ii) each eligible authority of a State, where the eligible authority was an agency at any time during the year to which the report relates; and
- (ad) for each State and for the Australian Capital Territory, the number and type of emergency service facilities located in that State or Territory that have been declared by the Minister during the year to which the report relates; and
- (ae) a summary of the information:
 - (i) that is included by the Ombudsman in the report made under subsection 84(1); and
 - (ii) that relates to the year to which the Minister's report relates; and
- (b) such other information (if any) as is prescribed.

103A Annual report for 1999-2000

- (1) The annual report for 1999-2000 must include a review of the amendments made by the *Telecommunications (Interception) and Listening Device Amendment Act 1997* to this Act.
- (2) For the purposes of the review, the Minister must arrange for a public notice, in plain English, to be published in at least one daily newspaper circulating in each State and Territory, calling for submissions from the public on the operation of amendments providing for the issuing of warrants by nominated AAT members, and including an address to which submissions may be sent.

103B Deferral of inclusion of information in report

Scope

- (1) This section applies to information:
 - (a) included in a report submitted to the Minister:
 - (i) under section 84 by the Ombudsman in relation to a Commonwealth agency; or
 - (ii) under section 94 by the chief officer of a Commonwealth agency; or

- (iii) under section 96 by the chief officer of an eligible authority of a State; and
- (b) that the Minister would, apart from this section, be required to include in the next Ministerial report.

Exclusion of information

- (2) If the chief officer of the Commonwealth agency or eligible authority is satisfied that the information is Part 5.3 information, the chief officer must advise the Minister in writing not to include the information in the next Ministerial report.
- (3) If the Minister is satisfied, on the advice of the chief officer, that the information is Part 5.3 information, the Minister must:
 - (a) notify the chief officer in writing; and
 - (b) not include the information in any Ministerial report until the Minister decides otherwise under subsection (5).

Inclusion of information in subsequent report

- (4) If the information has not been included in a Ministerial report because of subsection (3), the chief officer must, before the Minister prepares the next Ministerial report:
 - (a) reconsider whether the information is Part 5.3 information; and
 - (b) if the chief officer is satisfied that the information is not Part 5.3 information—advise the Minister in writing to include the information in the next Ministerial report.
- (5) If the Minister is satisfied, on the advice of the chief officer, that the information is not Part 5.3 information, the Minister must:
 - (a) notify the chief officer in writing; and
 - (b) include the information in the next Ministerial report.

Definitions

- (6) In this section:

Chapter 2 Interception of telecommunications

Part 2-8 Reports about interceptions under Parts 2-3 and 2-5

Division 2 Reports by the Minister

Section 103B

Ministerial report means a report the Minister prepares under this Division.

Part 5.3 information means information that, if made public, could reasonably be expected to enable a reasonable person to conclude that:

- (a) a Part 5.3 warrant is likely to be, or is not likely to be, in force in relation to a telecommunications service used, or likely to be used, by a particular person; or
- (b) a Part 5.3 warrant is likely to be, or is not likely to be, in force in relation to a particular person.

Division 3—Provisions about annual reports

104 Annual reports

- (1) The Minister shall cause a copy of a report under section 93 or Division 2 to be laid before each House of the Parliament within 15 sitting days of that House after the Minister receives the report, or the report is prepared, as the case may be.
- (2) A report under section 93 or Division 2 shall not be made in a manner that is likely to enable the identification of a person.
- (3) For the purposes of section 34C of the *Acts Interpretation Act 1901*, a report that section 93 or Division 2 requires to be given or prepared as soon as practicable after 30 June in a calendar year shall be deemed to be a periodic report that this Act requires a person to furnish to the Minister and that relates to the administration of Part 2-3, or Parts 2-5, 2-6 and 2-7, as the case may be, during the year ending on that 30 June.

Part 2-9—Offences

105 Contravention of section 7 or 63

- (1) A person who contravenes subsection 7(1) or section 63 is guilty of an offence against that subsection or section.
- (2) An offence against subsection 7(1) or section 63 is an indictable offence and, subject to this section, is punishable on conviction by imprisonment for a period not exceeding 2 years.
- (3) Notwithstanding that an offence against subsection 7(1) or section 63 is an indictable offence, a court of summary jurisdiction may hear and determine proceedings in respect of such an offence if, and only if:
 - (a) the proceedings are brought in the name of the Attorney-General or the Director of Public Prosecutions;
 - (b) the defendant and the prosecutor consent; and
 - (c) the court is satisfied that it is proper for the court to hear and determine proceedings in respect of the offence.
- (4) Where, in accordance with subsection (3), a court of summary jurisdiction convicts a person of an offence against subsection 7(1) or section 63, the penalty that the court may impose is imprisonment for a period not exceeding 6 months.
- (5) Section 15.1 (extended geographical jurisdiction—category A) of the *Criminal Code* applies to an offence against subsection 7(1) or section 63.

106 Obstruction

- (1) A person shall not obstruct or hinder a person acting under a warrant.

Penalty: Imprisonment for 6 months.

Section 107

- (2) Subsection (1) does not apply if the person obstructing or hindering has a reasonable excuse.

Note: A defendant bears an evidential burden in relation to the matter in subsection (2) (see subsection 13.3(3) of the *Criminal Code*).

107 Offences relating to inspections under Part 2-7

- (1) A person shall not refuse or fail:
- (a) to attend before a person;
 - (b) to furnish information; or
 - (c) to answer a question;
- when required under section 87 to do so.

Penalty: Imprisonment for 6 months.

- (2) A person shall not:
- (a) intentionally obstruct, hinder or resist a person in connection with the performance or exercise of the Ombudsman's functions or powers under Part 2-7; or
 - (b) give to an inspecting officer, in connection with an inspection under Part 2-7, information or a statement that the first-mentioned person knows to be false or misleading in a material particular.

Penalty: Imprisonment for 6 months.

- (3) Subsection (1) and paragraph (2)(a) do not apply if the person first mentioned in subsection (1) or (2) has a reasonable excuse.

Note: A defendant bears an evidential burden in relation to the matter in subsection (3) (see subsection 13.3(3) of the *Criminal Code*).

Section 107A

Part 2-10—Civil remedies

107A Civil remedies—unlawful interception or communication

When section applies

- (1) This section applies to an interception of a communication passing over a telecommunications system if the interception was in contravention of subsection 7(1).

Aggrieved person

- (2) For the purposes of this section, a person is an **aggrieved person** if, and only if:
- (a) the person was a party to the communication; or
 - (b) the communication was made on the person's behalf.

Interception—civil court remedy

- (3) If a person (in this subsection called the **defendant**):
- (a) so intercepted the communication; or
 - (b) did an act or thing referred to in paragraph 7(1)(b) or (c) in relation to the interception;

the Federal Court of Australia or a court of a State or Territory may, on the application of an aggrieved person, grant the aggrieved person remedial relief in respect of the interception by making such orders against the defendant as the court considers appropriate.

Note: Paragraphs 7(1)(b) and (c) deal with the authorisation or enabling of interception etc.

Communication—civil court remedy

- (4) If:
- (a) information was obtained by intercepting the communication; and

- (b) a person (in this subsection called the *defendant*) communicated the information to another person in contravention of section 63;

the Federal Court of Australia or a court of a State or Territory may, on the application of an aggrieved person, grant the aggrieved person remedial relief in respect of the communication of the information by making such orders against the defendant as the court considers appropriate.

Interception—criminal court remedy

- (5) If a court convicts a person (in this subsection called the *defendant*) of an offence against subsection 7(1) constituted by:
- (a) the interception; or
 - (b) the doing of an act or thing referred to in paragraph 7(1)(b) or (c) in relation to the interception;

the court may, on the application of an aggrieved person, grant the aggrieved person remedial relief in respect of the interception by making such orders against the defendant as the court considers appropriate.

Note: Paragraphs 7(1)(b) and (c) deal with the authorisation or enabling of interception etc.

Communication—criminal court remedy

- (6) If:
- (a) information was obtained by intercepting the communication; and
 - (b) the information was communicated to a person in contravention of section 63; and
 - (c) a court convicts a person (in this subsection called the *defendant*) of an offence against section 63 constituted by the communication of the information;

the court may, on the application of an aggrieved person, grant the aggrieved person remedial relief in respect of the communication of the information by making such orders against the defendant as the court considers appropriate.

Section 107A

Orders

- (7) Without limiting the orders that may be made under this section against a person (in this subsection called the *defendant*) in respect of a particular interception or a particular communication of information, a court may make an order of one or more of the following kinds:
- (a) an order declaring the interception or communication, as the case requires, to have been unlawful;
 - (b) an order that the defendant pay to the aggrieved person such damages as the court considers appropriate;
 - (c) an order in the nature of an injunction (including a mandatory injunction);
 - (d) an order that the defendant pay to the aggrieved person an amount not exceeding the amount that, in the opinion of the court, represents the total gross income derived by the defendant as a result of the interception or communication, as the case requires.

Terms etc. of orders

- (8) Without limiting the orders that may be made by a court under this section, an order may:
- (a) include such provisions as the court considers necessary for the purposes of the order; and
 - (b) be made either unconditionally or subject to such terms and conditions as the court determines.

Injunctive relief—variation etc.

- (9) A court may revoke or vary an order in the nature of an injunction made by the court under this section.

Punitive damages

- (10) A reference in paragraph (7)(b) to damages includes a reference to damages in the nature of punitive damages.

Minor irregularities in warrants etc.

- (11) Despite subsection (1) of this section, this section does not apply to an interception that contravenes subsection 7(1) only because of a defect or irregularity (other than a substantial defect or irregularity):
- (a) in, or in connection with the issue of, a document purporting to be a warrant; or
 - (b) in connection with the execution of a warrant, or the purported execution of a document purporting to be a warrant.

107B Limitation periods etc.

Interception—civil court remedy

- (1) An application under subsection 107A(3) for the grant of remedial relief in respect of an interception is to be made within 6 years after the end of the interception.

Communication—civil court remedy

- (2) An application under subsection 107A(4) for the grant of remedial relief in respect of a communication of information is to be made within 6 years after the communication.

Criminal court remedies

- (3) An application under subsection 107A(5) or (6) for the grant of remedial relief is not subject to any limitation period, but must be made as soon as practicable after the conviction concerned.

107C No limitation on other liability

No limitation

- (1) This Part does not limit any liability (whether criminal or civil) that a person has under any other provision of this Act or under any other law.

Section 107D

Remedial relief even if defendant convicted of offence

- (2) An application under subsection 107A(3) or (4) may be made even if the defendant referred to in that subsection has been convicted of an offence under, or arising out of, this Act.

107D Concurrent operation of State and Territory laws

This Part is not intended to exclude or limit the operation of a law of a State or Territory that is capable of operating concurrently with this Part.

107E State or Territory courts—jurisdictional limits

This Part does not enable an inferior court of a State or Territory to grant remedial relief of a kind that the court is unable to grant under the law of that State or Territory.

107F Extended meaning of *conviction*—orders under section 19B of the *Crimes Act 1914*

A reference in this Part to the conviction of a person of an offence includes a reference to the making of an order under section 19B of the *Crimes Act 1914* in relation to a person in respect of an offence.

Note: Section 19B of the *Crimes Act 1914* empowers a court that has found a person to have committed an offence to take action without proceeding to record a conviction.

Chapter 3—Preserving and accessing stored communications

Part 3-1A—Preserving stored communications

Division 1—Outline of this Part

107G Outline of this Part

This Part establishes a system of preserving certain stored communications that are held by a carrier. The purpose of the preservation is to prevent the communications from being destroyed before they can be accessed under certain warrants issued under this Act.

Under the system, certain agencies can give a preservation notice to a carrier requiring the carrier to preserve all stored communications that the carrier holds that relate to the person or telecommunications service specified in the notice. The carrier will breach its obligations under section 313 of the *Telecommunications Act 1997* if it does not comply with the notice.

There are 2 types of preservation notices: domestic preservation notices (which cover stored communications that might relate either to a contravention of certain Australian laws or to security) and foreign preservation notices (which cover stored communications that might relate to a contravention of certain foreign laws or to certain international offences).

Division 2 deals with domestic preservation notices. There are 2 kinds of domestic preservation notices:

- (a) historic domestic preservation notices, which cover stored communications held by the carrier on a particular day; and

Section 107G

- (b) ongoing domestic preservation notices, which cover stored communications held by the carrier in a particular 30-day period.

An issuing agency (which is a criminal law-enforcement agency, or the Organisation, for an historic domestic preservation notice, and a criminal law-enforcement agency that is an interception agency, or the Organisation, for an ongoing domestic preservation notice) can only give a domestic preservation notice if the conditions in section 107J are satisfied. There are certain grounds on which the notice must be revoked (see section 107L).

Division 3 deals with foreign preservation notices. Foreign preservation notices, like historic domestic preservation notices, cover stored communications held by the carrier on a particular day. Only the Australian Federal Police can give a foreign preservation notice to a carrier and it can only do so if a foreign country, the International Criminal Court or a War Crimes Tribunal has made a request for the preservation in accordance with section 107P. There are certain grounds on which the notice must be revoked (see section 107R).

Division 4 has miscellaneous provisions relating to both domestic and foreign preservation notices (such as provisions about the giving of evidentiary certificates by carriers and issuing agencies).

The Ombudsman has functions in relation to preservation notices given by issuing agencies (other than the Organisation) and the Inspector-General of Intelligence and Security has functions in relation to preservation notices given by the Organisation.

Division 2—Domestic preservation notices

107H Domestic preservation notices

- (1) An issuing agency may give a carrier a written notice (a *domestic preservation notice*) requiring the carrier to preserve, while the notice is in force, all stored communications that:
 - (a) relate to the person or telecommunications service specified in the notice; and
 - (b) the carrier holds at any time during:
 - (i) the period that starts at the time the carrier receives the notice and ends at the end of the day the carrier receives the notice (in which case the notice is an *historic domestic preservation notice*); or
 - (ii) the period that starts at the time the carrier receives the notice and ends at the end of the 29th day after the day the carrier receives the notice (in which case the notice is an *ongoing domestic preservation notice*).
- (2) However, the agency can only give the notice if the conditions in subsection 107J(1) or (2) are satisfied.
- (3) In the notice, the agency can only specify:
 - (a) one person; or
 - (b) one or more telecommunications services; or
 - (c) one person and one or more telecommunications services.

107J Conditions for giving domestic preservation notices

Notices given by criminal law-enforcement agencies

- (1) A domestic preservation notice may be given under subsection 107H(1) if:
 - (a) the issuing agency is:
 - (i) for an historic domestic preservation notice—a criminal law-enforcement agency; and

Section 107J

- (ii) for an ongoing domestic preservation notice—a criminal law-enforcement agency that is an interception agency; and
- (b) the agency is investigating a serious contravention; and
- (c) the agency considers that there are reasonable grounds for suspecting that, in the relevant period for the notice, there are stored communications in existence, or stored communications might come into existence, that:
 - (i) might assist in connection with the investigation; and
 - (ii) relate to the person or telecommunications service specified in the notice; and
- (d) the agency intends that if, at a later time, the agency considers that the stored communications would be likely to assist in connection with the investigation, then the agency will apply for a Part 2-5 warrant or a stored communications warrant to access those communications; and
- (e) for an ongoing domestic preservation notice—there is not another ongoing domestic preservation notice in force that:
 - (i) was given by the agency to the same carrier; and
 - (ii) specifies the same person or telecommunications service.

Notices given by the Organisation

- (2) A domestic preservation notice may be given under subsection 107H(1) if:
 - (a) the issuing agency is the Organisation; and
 - (b) the Organisation considers that there are reasonable grounds for suspecting that, in the relevant period for the notice, there are stored communications in existence, or stored communications might come into existence, that:
 - (i) might assist the Organisation in carrying out its function of obtaining intelligence relating to security; and
 - (ii) relate to the person or telecommunications service specified in the notice; and

- (c) the Organisation intends that if, at a later time, the Organisation considers that the stored communications would be likely to assist in carrying out that function, then the Director-General of Security will request a Part 2-2 warrant to access those communications; and
- (d) for an ongoing domestic preservation notice—there is not another ongoing domestic preservation notice in force that:
 - (i) was given by the Organisation to the same carrier; and
 - (ii) specifies the same person or telecommunications service.

107K When a domestic preservation notice is in force

A domestic preservation notice:

- (a) comes into force when the carrier receives it; and
- (b) ceases to be in force at the earliest of the following times:
 - (i) the end of the period of 90 days, starting on the day the carrier receives it;
 - (ii) if the notice is revoked under section 107L—when the carrier receives notice of the revocation;
 - (iii) if a Part 2-5 warrant or stored communications warrant authorising access to the stored communications covered by the notice is issued in relation to the issuing agency—when the warrant ceases to be in force;
 - (iv) if a Part 2-2 warrant authorising access to the stored communications covered by the notice is issued in relation to the issuing agency—the end of the period of 5 days after the day the warrant was issued.

107L Revoking a domestic preservation notice

Discretionary revocation

- (1) An issuing agency that has given a domestic preservation notice may revoke the notice at any time.

Section 107M

Mandatory revocation

- (2) An issuing agency that has given a domestic preservation notice must revoke the notice if:
- (a) if the issuing agency is a criminal law-enforcement agency (including an interception agency):
 - (i) the condition in paragraph 107J(1)(b) or (c) is no longer satisfied; or
 - (ii) the agency decides not to apply for a Part 2-5 warrant or stored communications warrant to access the stored communications covered by the notice; or
 - (b) if the issuing agency is the Organisation:
 - (i) the condition in paragraph 107J(2)(b) is no longer satisfied; or
 - (ii) the Organisation is satisfied that the Director-General of Security will not request a Part 2-2 warrant to access the stored communications covered by the notice.

Revocation effected by giving revocation notice

- (3) A domestic preservation notice is revoked by the issuing agency giving the carrier to whom it was given written notice of the revocation.

107M Persons who act on the issuing agency's behalf

Historic domestic preservation notices

- (1) An historic domestic preservation notice may only be given or revoked on behalf of an issuing agency by:
- (a) if the issuing agency is a criminal law-enforcement agency—a person who may, under section 110, apply on the agency's behalf for a stored communications warrant to access the stored communications covered by the notice; and
 - (b) if the issuing agency is the Organisation—a certifying person.

Ongoing domestic preservation notices

- (2) An ongoing domestic preservation notice may only be given on behalf of an issuing agency by:
- (a) if the issuing agency is a criminal law-enforcement agency that is an interception agency—an authorised officer of the agency; and
 - (b) if the issuing agency is the Organisation—the Director-General of Security.
- (3) An ongoing domestic preservation notice may only be revoked on behalf of an issuing agency by:
- (a) if the issuing agency is a criminal law-enforcement agency that is an interception agency—an authorised officer of the agency; and
 - (b) if the issuing agency is the Organisation—a certifying person.

Division 3—Foreign preservation notices

107N When a foreign preservation notice can be given

- (1) If the Australian Federal Police receives a request in accordance with section 107P, the Australian Federal Police must give the carrier to which the request relates a written notice (a ***foreign preservation notice***) requiring the carrier to preserve, while the notice is in force, all stored communications that:
 - (a) relate to the person or telecommunications service specified in the notice; and
 - (b) the carrier holds at any time during the period that starts at the time the carrier receives the notice and ends at the end of the day the carrier receives the notice.
- (2) In the notice, the Australian Federal Police can only specify:
 - (a) one person; or
 - (b) one or more telecommunications services; or
 - (c) one person and one or more telecommunications services.

107P Condition for giving a foreign preservation notice

- (1) An entity mentioned in the following table may request the Australian Federal Police to arrange for the preservation of stored communications that:
 - (a) relate to a specified person or specified telecommunications service; and
 - (b) are held by a carrier; and
 - (c) are relevant to an investigation, investigative proceeding, or proceeding relating to a serious foreign contravention;if the entity intends to make a request (an ***access request***) under a provision mentioned in the table to the Attorney-General to arrange for access to those stored communications.

Requesting access to stored communications

Item	This entity:	May make an access request under:
1	a foreign country	paragraph 15B(d) of the <i>Mutual Assistance in Criminal Matters Act 1987</i>
2	the International Criminal Court	paragraph 78A(b) of the <i>International Criminal Court Act 2002</i>
3	a War Crimes Tribunal	paragraph 34A(b) of the <i>International War Crimes Tribunals Act 1995</i>

- (2) The request by the entity to the Australian Federal Police must:
- (a) be in writing; and
 - (b) name the entity or the entity's authority concerned with the serious foreign contravention; and
 - (c) specify the serious foreign contravention that is the subject of the investigation, investigative proceeding or proceeding; and
 - (d) specify information identifying the stored communications to be preserved and the relationship between those communications and the serious foreign contravention; and
 - (e) specify any information the entity has that identifies the carrier that holds the stored communications; and
 - (f) if the stored communications relate to a specified person—specify any information the entity has that identifies the telecommunications service to which the stored communications relate; and
 - (g) specify the reasons why the stored communications need to be preserved; and
 - (h) specify that the entity intends to make an access request for the stored communications.

107Q When a foreign preservation notice is in force

A foreign preservation notice:

- (a) comes into force when the carrier receives it; and
- (b) ceases to be in force at the earlier of the following times:

Section 107R

- (i) if the notice is revoked under section 107R—when the carrier receives notice of the revocation;
- (ii) if a stored communications warrant authorising access to the stored communications covered by the notice is issued as a result of the access request—when the warrant ceases to be in force.

107R Revoking a foreign preservation notice

(1) If:

- (a) an entity requests under section 107P the Australian Federal Police to arrange for the preservation of stored communications that are held by a carrier; and
- (b) in response to the request, the Australian Federal Police gives a foreign preservation notice to the carrier in relation to those stored communications under subsection 107N(1); and
- (c) during the period of 180 days starting on the day the carrier was given the notice, the entity did not make an access request to the Attorney-General to arrange for access to those communications;

then the Australian Federal Police must, by the third working day after the end of that period, revoke the preservation notice by giving the carrier to whom it was given written notice of the revocation.

(2) If:

- (a) an entity requests under section 107P the Australian Federal Police to arrange for the preservation of stored communications that are held by a carrier; and
- (b) in response to the request, the Australian Federal Police gives a foreign preservation notice to the carrier in relation to those stored communications under subsection 107N(1); and
- (c) the entity makes an access request to the Attorney-General to arrange for access to those communications; and
- (d) the Attorney-General refuses that access request;

then the Australian Federal Police must, by the third working day after it is notified of the refusal, revoke the preservation notice by

giving the carrier to whom it was given written notice of the revocation.

(3) If:

- (a) an entity requests under section 107P the Australian Federal Police to arrange for the preservation of stored communications that are held by a carrier; and
- (b) in response to the request, the Australian Federal Police gives a foreign preservation notice to the carrier in relation to those stored communications under subsection 107N(1); and
- (c) the entity withdraws the request;

then the Australian Federal Police must, by the third working day after it is notified of the withdrawal, revoke the preservation notice by giving the carrier to whom it was given written notice of the revocation.

107S Persons who act on the AFP's behalf

A foreign preservation notice must be given or revoked on behalf of the Australian Federal Police by an authorised officer of the Australian Federal Police.

Division 4—Provisions relating to preservation notices

107T Evidentiary certificates relating to actions by carriers

(1) The following:

- (a) the Managing Director of a carrier or a body corporate of which the carrier is a subsidiary;
- (b) the secretary of a carrier or a body corporate of which the carrier is a subsidiary;
- (c) an employee of a carrier authorised in writing for the purposes of this paragraph by a person referred to in paragraph (a) or (b);

may issue a written certificate signed by him or her setting out such facts as he or she considers relevant with respect to acts or things done by, or in relation to, employees of the carrier in order to comply with a preservation notice.

(2) A document purporting to be a certificate issued under subsection (1) and purporting to be signed by a person referred to in paragraph (a), (b) or (c) of that subsection:

- (a) is to be received in evidence in an exempt proceeding without further proof; and
- (b) in an exempt proceeding, is conclusive evidence of the matters stated in the document.

(3) For the purposes of this section, the question whether a body corporate is a subsidiary of another body corporate is to be determined in the same manner as the question is determined under the *Corporations Act 2001*.

107U Evidentiary certificates relating to actions by issuing agencies

(1) A certifying official of an issuing agency may issue a written certificate signed by him or her setting out such facts as he or she considers relevant with respect to anything done by an officer or staff member of the agency in connection with a preservation notice.

- (2) A document purporting to be a certificate issued under this section by a certifying official of an issuing agency and purporting to be signed by him or her:
- (a) is to be received in evidence in an exempt proceeding without further proof; and
 - (b) in an exempt proceeding, is prima facie evidence of the matters stated in the document.

107V Certified copies of preservation notices

A document certified in writing by a certifying official of an issuing agency to be a true copy of a preservation notice is to be received in evidence in an exempt proceeding as if it were the original preservation notice.

107W How notices are to be given to carriers

For the purposes of this Part:

- (a) a preservation notice; or
 - (b) a revocation notice under section 107L or 107R;
- may only be given to a carrier by giving it to an authorised representative of the carrier.

Part 3-1—Prohibition on access to stored communications

108 Stored communications not to be accessed

- (1) A person commits an offence if:
- (a) the person:
 - (i) accesses a stored communication; or
 - (ii) authorises, suffers or permits another person to access a stored communication; or
 - (iii) does any act or thing that will enable the person or another person to access a stored communication; and
 - (b) the person does so with the knowledge of neither of the following:
 - (i) the intended recipient of the stored communication;
 - (ii) the person who sent the stored communication.

Penalty: Imprisonment for 2 years or 120 penalty units, or both.

Note: This section does not prohibit accessing of communications, that are no longer passing over a telecommunications system, from the intended recipient or from a telecommunications device in the possession of the intended recipient.

- (1A) Without limiting paragraph (1)(b), a person is taken for the purposes of that paragraph to have knowledge of an act referred to in paragraph (1)(a) if written notice of an intention to do the act is given to the person.

Note: For giving notice, see section 28A of the *Acts Interpretation Act 1901*.

- (2) Subsection (1) does not apply to or in relation to:
- (a) accessing a stored communication under a stored communications warrant; or
 - (b) accessing a stored communication under an interception warrant; or

- (c) accessing a stored communication under a computer access warrant issued under section 25A of the *Australian Security Intelligence Organisation Act 1979*; or
- (ca) accessing a stored communication under an authorisation given under a warrant in accordance with section 27E of the *Australian Security Intelligence Organisation Act 1979*; or
- (cb) accessing a stored communication under a general computer access warrant; or
- (cba) accessing a stored communication under a data disruption warrant; or
- (cc) an act or thing done in compliance with an international production order (within the meaning of Schedule 1); or
- (cd) accessing a stored communication under a network activity warrant; or
- (d) an act or thing done by an employee of a carrier in the course of his or her duties for or in connection with:
 - (i) the installation of any line, or the installation of any equipment, used or intended for use in connection with a telecommunications service; or
 - (ii) the operation or maintenance of a telecommunications system; or
 - (iii) the identifying or tracing of any person who has contravened, or is suspected of having contravened or being likely to contravene, a provision of Part 10.6 of the *Criminal Code*;
if it is reasonably necessary for the employee to do that act or thing in order to perform those duties effectively; or
- (e) accessing a stored communication by another person lawfully engaged in duties relating to the installation, connection or maintenance of equipment or a line, if it is reasonably necessary for the person to access the communication in order to perform those duties effectively; or
- (f) accessing a stored communication by a person lawfully engaged in duties relating to the installation, connection or maintenance of equipment used, or to be used, for accessing stored communications under:

Section 108

- (ia) preservation notices; or
- (i) stored communications warrants; or
- (ii) interception warrants; or
- (iii) computer access warrants issued under section 25A of the *Australian Security Intelligence Organisation Act 1979*; or
- (iv) authorisations given under warrants in accordance with section 27E of the *Australian Security Intelligence Organisation Act 1979*; or
- (g) accessing a stored communication if the access results from, or is incidental to, action taken by an ASIO employee, in the lawful performance of his or her duties, for the purpose of:
 - (i) discovering whether a listening device is being used at, or in relation to, a particular place; or
 - (ii) determining the location of a listening device; or
- (ga) accessing a stored communication if the access results from, or is incidental to, action taken by an ASIO affiliate, in accordance with the contract, agreement or other arrangement under which the ASIO affiliate is performing functions or services for the Organisation, for the purpose of:
 - (i) discovering whether a listening device is being used at, or in relation to, a particular place; or
 - (ii) determining the location of a listening device; or
- (h) accessing a stored communication by an officer or staff member of the Australian Communications and Media Authority engaged in duties relating to enforcement of the *Spam Act 2003*.

Note: A defendant bears an evidential burden in relation to the matter in subsection (2) (see subsection 13.3(3) of the *Criminal Code*).

- (3) For the purposes of paragraph (2)(b), access to a stored communication is taken to be under an interception warrant if, and only if, the warrant would have authorised interception of the communication if it were still passing over a telecommunications system.

- (4) In determining, for the purposes of paragraphs (2)(d) and (e), whether an act or thing done by a person was reasonably necessary in order for the person to perform his or her duties effectively, a court is to have regard to such matters (if any) as are specified in, or ascertained in accordance with, the regulations.

Note: The civil remedy provisions in Part 3-7 may apply to a contravention of this section.

Part 3-2—Access by the Organisation to stored communications

109 Access to stored communications under Part 2-2 warrants

In addition to authorising interception of communications, a Part 2-2 warrant also authorises a person to access a stored communication if:

- (a) the warrant would have authorised interception of the communication if it were still passing over a telecommunications system; and
- (b) the person is approved under section 12 in respect of the warrant.

Part 3-3—Access by criminal law-enforcement agencies to stored communications

Division 1—Applications for warrants

110 Criminal law-enforcement agencies may apply for stored communications warrants

- (1) A criminal law-enforcement agency may apply to an issuing authority for a stored communications warrant in respect of a person.
- (2) The application must be made on the agency's behalf by:
 - (a) if the agency is referred to in subsection 39(2)—a person referred to in that subsection in relation to that agency; or
 - (b) otherwise:
 - (i) the chief officer of the agency; or
 - (ii) an officer of the agency (by whatever name called) who holds, or is acting in, an office or position in the agency nominated under subsection (3).
- (3) The chief officer of the agency may, in writing, nominate for the purposes of subparagraph (2)(b)(ii) an office or position in the agency that is involved in the management of the agency.
- (4) A nomination under subsection (3) is not a legislative instrument.

110A Meaning of *criminal law-enforcement agency*

- (1) Each of the following is a *criminal law-enforcement agency*:
 - (a) the Australian Federal Police;
 - (b) a Police Force of a State;
 - (c) the Australian Commission for Law Enforcement Integrity;
 - (d) the ACC;

Chapter 3 Preserving and accessing stored communications

Part 3-3 Access by criminal law-enforcement agencies to stored communications

Division 1 Applications for warrants

Section 110A

- (e) subject to subsection (1A), the Immigration and Border Protection Department;
 - (ea) the Australian Securities and Investments Commission;
 - (eb) the Australian Competition and Consumer Commission;
 - (f) the Crime Commission;
 - (g) the Independent Commission Against Corruption;
 - (h) the Law Enforcement Conduct Commission;
 - (i) the IBAC;
 - (j) the Crime and Corruption Commission;
 - (k) the Corruption and Crime Commission;
 - (l) the Independent Commissioner Against Corruption;
 - (m) subject to subsection (7), an authority or body for which a declaration under subsection (3) is in force.
- (1A) Paragraph (1)(e) applies to the Immigration and Border Protection Department only in connection with the investigation by that Department of a contravention of:
- (a) the *Customs Act 1901*; or
 - (b) the *Crimes Act 1914*; or
 - (c) the *Criminal Code*; or
 - (d) the *Environment Protection and Biodiversity Conservation Act 1999*; or
 - (e) Part 6 of the *Australian Border Force Act 2015*; or
 - (f) an Act prescribed in a legislative instrument made by the Minister for the purposes of this paragraph; or
 - (g) a provision of an Act, being a provision prescribed in a legislative instrument made by the Minister for the purposes of this paragraph.
- Note: See also section 110B.
- (2) The head of an authority or body may request the Minister to declare the authority or body to be a criminal law-enforcement agency.
- (3) The Minister may, by legislative instrument, declare:

- (a) an authority or body to be a criminal law-enforcement agency; and
 - (b) persons specified, or of a kind specified, in the declaration to be officers of the criminal law-enforcement agency for the purposes of this Act.
- (3A) The Minister may make the declaration whether or not the head of the authority or body has made a request under subsection (2).
- (3B) The Minister must not make the declaration unless the Minister is satisfied on reasonable grounds that the functions of the authority or body include investigating serious contraventions.
- (4) In considering whether to make the declaration, the Minister must have regard to:
- (b) whether access to stored communications, and the making of authorisations under section 180, would be reasonably likely to assist the authority or body in investigating serious contraventions; and
 - (c) whether the authority or body:
 - (i) is required to comply with the Australian Privacy Principles; or
 - (ii) is required to comply with a binding scheme that provides protection of personal information that meets the requirements of subsection (4A); or
 - (iii) has agreed in writing to comply with a scheme providing such protection of personal information, in relation to personal information disclosed to it under Chapter 3 or 4, if the declaration is made; and
 - (d) whether the authority or body proposes to adopt processes and practices that would ensure its compliance with the obligations of a criminal law-enforcement agency under Chapter 3, and the obligations of an enforcement agency under Chapter 4; and
 - (e) whether the Minister considers that the declaration would be in the public interest; and
 - (f) any other matter that the Minister considers relevant.

Section 110A

- (4A) For the purposes of subparagraphs (4)(c)(ii) and (iii), the protection of personal information provided by the scheme must:
- (a) be comparable to the protection provided by the Australian Privacy Principles; and
 - (b) include a mechanism for monitoring the authority's or body's compliance with the scheme; and
 - (c) include a mechanism that enables an individual to seek recourse if his or her personal information is mishandled.
- (5) In considering whether to make the declaration, the Minister may consult such persons or bodies as the Minister thinks fit. In particular, the Minister may consult the Privacy Commissioner and the Ombudsman.
- (6) The declaration may be subject to conditions.
- (7) Without limiting subsection (6), a condition may provide that the authority or body is not to exercise:
- (a) a power conferred on a criminal law-enforcement agency by or under a specified provision in Chapter 3; or
 - (b) a power conferred on an enforcement agency by or under a specified provision in Chapter 4.
- The authority or body is taken, for the purposes of this Act, not to be a criminal law-enforcement agency for the purposes of that provision in Chapter 3, or an enforcement agency for the purposes of that provision in Chapter 4, as the case requires.
- (8) The Minister may, by legislative instrument, revoke a declaration under subsection (3) relating to an authority or body if the Minister is no longer satisfied that the circumstances justify the declaration remaining in force.
- (9) The revocation under subsection (8) of a declaration relating to an authority or body does not affect the validity of:
- (a) a domestic preservation notice given by the authority or body; or
 - (b) a stored communications warrant issued to the authority or body; or

- (c) an authorisation made by an authorised officer of the authority or body under Division 4 of Part 4-1; that was in force immediately before the revocation took effect.
- (10) A declaration under subsection (3):
- (a) comes into force when it is made, or on such later day as is specified in the declaration; and
 - (b) ceases to be in force at the end of the period of 40 sitting days of a House of the Parliament after the declaration comes into force.
- (11) If a Bill is introduced into either House of the Parliament that includes an amendment of subsection (1), the Minister:
- (a) must refer the amendment to the Parliamentary Joint Committee on Intelligence and Security for review; and
 - (b) must not in that referral specify, as the period within which the Committee is to report on its review, a period that will end earlier than 15 sitting days of a House of the Parliament after the introduction of the Bill.

110B Declarations in relation to the Immigration and Border Protection Department

Provisions of Chapter 3 or 4 that do not apply to the Immigration and Border Protection Department

- (1) The Minister may, by legislative instrument, declare that:
- (a) a specified provision in Chapter 3 or 4, referring to a criminal law-enforcement agency, does not apply in relation to the Immigration and Border Protection Department; or
 - (b) a specified provision in Chapter 4, referring to an enforcement agency, does not apply in relation to the Immigration and Border Protection Department.

Provisions of Chapter 3 or 4 that have a limited application to the Immigration and Border Protection Department

- (2) The Minister may, by legislative instrument, declare that:

Section 111

- (a) a specified provision in Chapter 3 or 4, referring to a criminal law-enforcement agency, applies in relation to the Immigration and Border Protection Department only to the extent specified in the declaration; or
- (b) a specified provision in Chapter 4, referring to an enforcement agency, applies in relation to the Immigration and Border Protection Department only to the extent specified in the declaration.

111 Form of applications

- (1) The application must be in writing.
- (2) However, a person making the application on the agency's behalf may make the application by telephone if the person:
 - (a) is the chief officer of the agency or a person in relation to whom an authorisation by the chief officer is in force under subsection (3); and
 - (b) thinks it necessary, because of urgent circumstances, to make the application by telephone.
- (3) The chief officer of a criminal law-enforcement agency may, in writing, authorise persons (including classes of persons) for the purposes of subsection (2). However, each person must be entitled under section 110 to make applications on the agency's behalf.

112 Contents of written applications

The application must, if it is in writing, set out:

- (a) the name of the agency; and
- (b) the name of the person making the application on the agency's behalf.

113 Affidavits to accompany written applications

- (1) The application must, if it is in writing, be accompanied by an affidavit complying with this section.

- (2) The affidavit must set out the facts and other grounds on which the application is based.
- (3) Despite subsection (1), a written application may be accompanied by 2 or more affidavits that together set out each matter that, but for this subsection, this section would have required an affidavit accompanying the application to set out.

114 Information to be given on telephone applications

The information given to an issuing authority in connection with a telephone application to the issuing authority:

- (a) must include particulars of the urgent circumstances because of which the person making the application on the agency's behalf thinks it necessary to make the application by telephone; and
- (b) must include each matter that, if the application had been made in writing, section 112 or 113 would have required the application, or an affidavit accompanying it, to set out; and
- (c) must be given orally or in writing, as the issuing authority directs.

115 Giving further information to Judge

- (1) An issuing authority may require further information to be given in connection with an application to the issuing authority for a warrant.
- (2) The further information:
 - (a) must be given on oath if the application was made in writing; and
 - (b) must be given orally or otherwise, as the issuing authority directs.

Division 2—Issuing of warrants

116 Issuing of stored communications warrants

- (1) An issuing authority to whom a criminal law-enforcement agency has applied for a stored communications warrant in respect of a person may, in his or her discretion, issue such a warrant if satisfied, on the basis of the information given to him or her under this Part in connection with the application, that:
 - (a) Division 1 has been complied with in relation to the application; and
 - (b) in the case of a telephone application—because of urgent circumstances, it was necessary to make the application by telephone; and
 - (c) there are reasonable grounds for suspecting that a particular carrier holds stored communications:
 - (i) that the person has made; or
 - (ii) that another person has made and for which the person is the intended recipient; and
 - (d) information that would be likely to be obtained by accessing those stored communications under a stored communications warrant would be likely to assist in connection with:
 - (i) unless subparagraph (ii) applies—the investigation by the agency of a serious contravention in which the person is involved (including as a victim of the serious contravention); or
 - (ii) for an international assistance application—the investigation, investigative proceeding, or proceeding by the entity to which the application relates, of a serious foreign contravention to which the application relates and in which the person is involved (including as a victim of the serious foreign contravention); and

- (da) if the stored communications warrant is applied for in relation to a person who is the victim of the serious contravention—the person is unable to consent, or it is impracticable for the person to consent, to those stored communications being accessed; and
 - (e) in any case—having regard to the matters referred to in subsection (2) or (2A) (as the case requires), and to no other matters, the issuing authority should issue a warrant authorising access to such stored communications.
- (2) For an application other than an international assistance application, the matters to which the issuing authority must have regard are:
- (a) how much the privacy of any person or persons would be likely to be interfered with by accessing those stored communications under a stored communications warrant; and
 - (b) the gravity of the conduct constituting the serious contravention; and
 - (c) how much the information referred to in subparagraph (1)(d)(i) would be likely to assist in connection with the investigation; and
 - (d) to what extent methods of investigating the serious contravention that do not involve the use of a stored communications warrant in relation to the person have been used by, or are available to, the agency; and
 - (e) how much the use of such methods would be likely to assist in connection with the investigation by the agency of the serious contravention; and
 - (f) how much the use of such methods would be likely to prejudice the investigation by the agency of the serious contravention, whether because of delay or for any other reason.
- (2A) For an international assistance application, the matters to which the issuing authority must have regard are:

Section 117

- (a) how much the privacy of any person or persons would be likely to be interfered with by accessing those stored communications under a stored communications warrant; and
 - (b) the gravity of the conduct constituting the serious foreign contravention; and
 - (c) how much the information referred to in subparagraph (1)(d)(ii) would be likely to assist in connection with the investigation, investigative proceeding, or proceeding, to the extent that this is possible to determine from information obtained from the entity to which the application relates.
- (3) The warrant may be issued in relation to the investigation of more than one serious contravention or serious foreign contravention, but cannot relate to both a serious contravention and a serious foreign contravention.

117 What stored communications warrants authorise

A stored communications warrant authorises persons approved under subsection 127(2) in respect of the warrant to access, subject to any conditions or restrictions that are specified in the warrant, a stored communication:

- (a) that was made by the person in respect of whom the warrant was issued; or
- (b) that another person has made and for which the intended recipient is the person in respect of whom the warrant was issued;

and that becomes, or became, a stored communication before the warrant is first executed in relation to the carrier that holds the communication.

118 Form and content of stored communications warrants

- (1) A stored communications warrant:
 - (a) must be in accordance with the prescribed form; and
 - (b) must be signed by the issuing authority who issues it.

- (2) A stored communications warrant may specify conditions or restrictions relating to accessing stored communications under the warrant.
- (3) A stored communications warrant must set out short particulars of each serious contravention or serious foreign contravention in relation to which the issuing authority issuing the warrant was satisfied, on the application for the warrant, as mentioned in subparagraph 116(1)(d)(i) or (ii), as the case may be.

119 Duration of stored communications warrants

- (1) A stored communications warrant remains in force:
 - (a) until it is first executed; or
 - (b) until the end of the period of 5 days after the day on which it was issued;whichever occurs sooner.
- (2) However, if the warrant relates to more than one telecommunications service and those services are not all operated by the same carrier, the warrant remains in force, to the extent that it relates to a telecommunications service operated by a particular carrier:
 - (a) until it is first executed in relation to a telecommunications service operated by that particular carrier; or
 - (b) until the end of the period of 5 days after the day on which it was issued;whichever occurs sooner.
- (3) An issuing authority must not vary a stored communications warrant by extending the period for which it is to be in force.
- (4) This section does not prevent the issue of a further warrant in respect of the person in respect of whom the warrant was issued.
- (5) However, if the further warrant relates to the same telecommunications service as the previous warrant, it must not be issued within 3 days after the day on which the previous warrant was executed or (if subsection (2) applies) was last executed.

Division 3—How warrants etc. are dealt with

120 Stored communications warrants issued on telephone applications

- (1) An issuing authority who issues a stored communications warrant on a telephone application:
 - (a) must, as soon as practicable after completing and signing the warrant:
 - (i) inform the person who made the application, on behalf of the criminal law-enforcement agency concerned, of the terms of the warrant, the day on which it was signed and the time at which it was signed; and
 - (ii) give the warrant to that person; and
 - (b) must keep a copy of the warrant.
- (2) A person who makes a telephone application on a criminal law-enforcement agency's behalf must, within one day after the day on which a warrant is issued on the application:
 - (a) cause each person who gave information to the issuing authority in connection with the application to swear an affidavit setting out the information so given by the person; and
 - (b) give to the issuing authority:
 - (i) the affidavit or affidavits; and
 - (ii) unless the applicant is the chief officer of the criminal law-enforcement agency—a copy of an authorisation by the chief officer under subsection 111(3) that was in force in relation to the applicant when the application was made.
- (3) An issuing authority may, by writing signed by him or her, revoke a warrant that he or she issued on a telephone application if satisfied that subsection (2) has not been complied with in relation to the warrant. If he or she does so, he or she must:

- (a) forthwith inform the person who made the application on the criminal law-enforcement agency's behalf, or the chief officer of the criminal law-enforcement agency, of the revocation; and
 - (b) give the instrument of revocation to that person, or to the chief officer, as soon as practicable.
- (4) The chief officer of that agency must, if another criminal law-enforcement agency is exercising authority under the warrant:
- (a) cause the chief officer of the other agency to be informed forthwith of the revocation; and
 - (b) cause a copy of the instrument of revocation to be given as soon as practicable to the chief officer of the other agency.

121 What happens when stored communications warrants are issued

The chief officer of the agency must cause:

- (a) an authorised representative of the carrier that holds the stored communications to which the warrant relates to be informed forthwith of the issue of the warrant; and
- (b) a copy of the warrant, certified in writing by a certifying officer of the agency to be a true copy of the warrant, to be given as soon as practicable to that authorised representative.

122 Revocation of stored communications warrants by chief officers

- (1) The chief officer of a criminal law-enforcement agency to which a stored communications warrant has been issued must, on being satisfied that the grounds on which the warrant was issued have ceased to exist:
- (a) cause the chief officer of any other criminal law-enforcement agency that is exercising authority under the warrant to be informed forthwith of the proposed revocation of the warrant; and
 - (b) by writing signed by him or her, revoke the warrant.

Section 123

- (2) The chief officer of a criminal law-enforcement agency may at any time, by writing signed by him or her, revoke a warrant issued to the agency after causing the chief officer of any other criminal law-enforcement agency that is exercising authority under the warrant to be informed forthwith that the chief officer proposes to revoke the warrant.
- (3) The chief officer of a criminal law-enforcement agency may delegate his or her power under subsection (2) to a certifying officer of the agency.
- (4) This section does not apply in relation to a warrant that has ceased to be in force.

123 What happens when stored communications warrants are revoked

- (1) Upon revoking a stored communications warrant, the chief officer of a criminal law-enforcement agency must cause the chief officer of any other criminal law-enforcement agency that is exercising authority under the warrant to be informed forthwith of the revocation.
- (2) If an authorised representative of a carrier has been informed, under section 121, of the issue of a stored communications warrant and that warrant is subsequently revoked, the chief officer of the criminal law-enforcement agency to which the warrant was issued must:
 - (a) cause that authorised representative to be informed forthwith of the revocation; and
 - (b) cause a copy of the instrument of revocation, certified in writing by a certifying officer to be a true copy of the instrument, to be given as soon as practicable to that authorised representative.

124 Access to additional telecommunications services under stored communications warrants

- (1) If:
-

- (a) an authorised representative of a carrier has been informed, under section 121, of the issue of a stored communications warrant; and
 - (b) it is proposed, under the warrant, to access stored communications that, immediately before they became stored communications, had passed over a telecommunications service operated by a carrier; and
 - (c) the service was not identified in the warrant;
- the chief officer must cause that authorised representative to be given, as soon as practicable, a description in writing of the service sufficient to identify it.
- (2) If:
- (a) an authorised representative of a carrier has been informed, under subsection (1) of the issue of a stored communications warrant; and
 - (b) the chief officer of the agency to which the warrant was issued, or a certifying officer of that agency, is satisfied that it is no longer necessary to access stored communications that, immediately before they became stored communications, had passed over that service;
- the chief officer or the certifying officer must cause:
- (c) that authorised representative to be informed forthwith of the fact; and
 - (d) confirmation in writing of the fact to be given as soon as practicable to that authorised representative.

Division 4—Provisions relating to execution of warrants

125 Entry into force of stored communications warrants

A stored communications warrant comes into force when it is issued.

126 Limit on authority conferred by warrant

A stored communications warrant does not authorise access to stored communications unless notification of the issue of the warrant has been received under section 121 by an authorised representative of the carrier holding the stored communications.

127 Exercise of authority conferred by warrant

- (1) The authority conferred by a stored communications warrant may only be exercised by a person in relation to whom an approval under subsection (2) is in force in relation to the warrant.
- (2) The chief officer of a criminal law-enforcement agency, or an officer of a criminal law-enforcement agency in relation to whom an appointment under subsection (3) is in force, may approve any of the following persons to exercise the authority conferred by warrants (or classes of warrants) issued to the agency:
 - (a) officers (or classes of officers) of the agency or another criminal law-enforcement agency;
 - (b) staff members (or classes of staff members) of the agency or another criminal law-enforcement agency.
- (3) The chief officer of a criminal law-enforcement agency may appoint in writing an officer of the agency to be an approving officer for the purposes of subsection (2).

128 Provision of technical assistance

- (1) Despite subsection 127(1), a designated officer, or an employee of a carrier, may provide technical assistance to an officer or staff member of a criminal law-enforcement agency who is exercising the authority conferred by a stored communications warrant.
- (2) For the purposes of subsection (1), the provision of technical assistance includes (but is not limited to):
 - (a) the doing of any act in connection with:
 - (i) the installation of equipment for the purposes of accessing stored communications in accordance with a stored communications warrant; or
 - (ii) the maintenance, testing or use of such equipment; or
 - (iii) the removal of such equipment; and
 - (b) the doing of any act involved in the accessing of a stored communication under a stored communications warrant, to the extent that the act is incidental to the doing of an act referred to in paragraph (a).
- (3) The chief officer of a criminal law-enforcement agency or a person who is an approving officer for a criminal law-enforcement agency under subsection 127(3) may, in writing, declare persons to be designated officers for the purposes of this section.

129 Evidentiary certificates relating to actions by carriers

- (1) The following:
 - (a) the Managing Director of a carrier or a body corporate of which the carrier is a subsidiary;
 - (b) the secretary of a carrier or a body corporate of which the carrier is a subsidiary;
 - (c) an employee of a carrier authorised in writing for the purposes of this paragraph by a person referred to in paragraph (a) or (b);may issue a written certificate signed by him or her setting out such facts as he or she considers relevant with respect to acts or things

Section 130

done by, or in relation to, employees of the carrier in order to enable a warrant to be executed.

- (2) A document purporting to be a certificate issued under subsection (1) and purporting to be signed by a person referred to in paragraph (a), (b) or (c) of that subsection:
 - (a) is to be received in evidence in an exempt proceeding without further proof; and
 - (b) in an exempt proceeding, is conclusive evidence of the matters stated in the document.
- (3) For the purposes of this section, the question whether a body corporate is a subsidiary of another body corporate is to be determined in the same manner as the question is determined under the *Corporations Act 2001*.

130 Evidentiary certificates relating to actions by criminal law-enforcement agencies

- (1) A certifying officer of a criminal law-enforcement agency may issue a written certificate signed by him or her setting out such facts as he or she considers relevant with respect to:
 - (a) anything done by an officer or staff member of the agency in connection with the execution of a stored communications warrant; or
 - (b) anything done by an officer or staff member of the agency in connection with:
 - (i) the communication by a person to another person of information obtained by the execution of such a warrant; or
 - (ii) the making use of such information; or
 - (iii) the making of a record of such information; or
 - (iv) the custody of a record of such information; or
 - (v) the giving in evidence of such information.

- (2) A document purporting to be a certificate issued under this section by a certifying officer of a criminal law-enforcement agency and to be signed by him or her:
- (a) is to be received in evidence in an exempt proceeding without further proof; and
 - (b) in an exempt proceeding, is prima facie evidence of the matters stated in the document.

131 Certified copies of stored communications warrants

A document certified in writing by a certifying officer of a criminal law-enforcement agency to be a true copy of a stored communications warrant is to be received in evidence in an exempt proceeding as if it were the original warrant.

132 Obstruction

- (1) A person commits an offence if the person obstructs or hinders another person acting under a stored communications warrant.
- Penalty: Imprisonment for 6 months or 30 penalty units, or both.
- (2) Subsection (1) does not apply if the person obstructing or hindering has a reasonable excuse.

Note: A defendant bears an evidential burden in relation to the matter in subsection (2) (see subsection 13.3(3) of the *Criminal Code*).

Part 3-4—Dealing with accessed information etc.

Division 1—Prohibition on dealing with accessed information etc.

133 No dealing with accessed information etc.

- (1) A person commits an offence if:
- (a) the person:
 - (i) communicates information to another person; or
 - (ii) makes use of information; or
 - (iii) makes a record of information; or
 - (iv) gives information in evidence in a proceeding; and
 - (b) the information is:
 - (i) lawfully accessed information; or
 - (ii) information obtained by accessing a stored communication in contravention of subsection 108(1);
or
 - (iia) preservation notice information; or
 - (iii) stored communications warrant information.

Penalty: Imprisonment for 2 years or 120 penalty units, or both.

- (2) Subsection (1) does not apply to conduct permitted under this Part or section 299.

Note 1: A defendant bears an evidential burden in relation to the matter in subsection (2) (see subsection 13.3(3) of the *Criminal Code*).

Note 2: The civil remedy provisions in Part 3-7 may apply to a contravention of this section.

Division 2—Permitted dealings with accessed information

134 Dealing in preservation notice information or stored communications warrant information

A person may, for the purposes of Part 3-1A, 3-2, 3-3, 3-5 or 3-6 or Chapter 4A:

- (a) communicate preservation notice information or stored communications warrant information to another person; or
- (b) make use of preservation notice information or stored communications warrant information; or
- (c) make a record of preservation notice information or stored communications warrant information; or
- (d) give preservation notice information or stored communications warrant information in evidence in a proceeding.

135 Dealing in information by employees of carriers

Communicating information to the appropriate criminal law-enforcement agency

- (1) An employee of a carrier may communicate information obtained by accessing stored communications under a stored communications warrant to:
 - (a) the officer of the criminal law-enforcement agency who applied for the warrant on the agency's behalf; or
 - (b) an officer of the agency in relation to whom an authorisation under subsection (2) by the chief officer of the agency is in force in relation to the warrant.
- (2) The chief officer of a criminal law-enforcement agency may authorise in writing officers, or classes of officers, of the agency to receive information obtained by accessing stored communications under stored communications warrants, or classes of such warrants, issued to the agency.

Section 135

Information relating to operation of networks etc.

- (3) An employee of a carrier may communicate or make use of, or cause to be communicated, lawfully accessed information or information that has been obtained by accessing a stored communication in contravention of subsection 108(1) if:
- (a) the employee does so in the performance of his or her duties as such an employee; and
 - (b) the information relates to:
 - (i) the operation or maintenance of a telecommunications network operated by the carrier; or
 - (ii) the supply of services by the carrier by means of a telecommunications network.
- (4) An employee of a carrier may communicate or cause to be communicated to another carrier, or to an employee of another carrier, lawfully accessed information or information that has been obtained by accessing a stored communication in contravention of subsection 108(1) if:
- (a) the communication of the information is for the purpose of the carrying on by the other carrier of its business relating to the supply of services by means of a telecommunications network operated by the other carrier; and
 - (b) the information relates to:
 - (i) the operation or maintenance of a telecommunications network operated by the other carrier; or
 - (ii) the supply of services by the other carrier by means of a telecommunications network.

Preservation notice information

- (4A) An employee of a carrier may, in the performance of his or her duties as such an employee, communicate or make use of, or cause to be communicated, preservation notice information if:
- (a) the employee does so in the performance of his or her duties as such an employee; and

- (b) the information is reasonably necessary to enable the carrier to comply with the preservation notice.
- (4B) An employee of a carrier may communicate or cause to be communicated to another carrier, or to an employee of another carrier, preservation notice information if the information is reasonably necessary to enable the carrier to comply with the preservation notice.

Stored communications warrant information

- (5) An employee of a carrier may, in the performance of his or her duties as such an employee, communicate or make use of, or cause to be communicated, stored communications warrant information if:
- (a) the employee does so in the performance of his or her duties as such an employee; and
 - (b) the information is reasonably necessary to enable access to a stored communication under a stored communications warrant.
- (6) An employee of a carrier may communicate or cause to be communicated to another carrier, or to an employee of another carrier, stored communications warrant information if the information is reasonably necessary to enable access to a stored communication under a stored communications warrant.

136 Dealing in connection with Organisation's functions

- (1) A person may, in connection with the performance by the Organisation of its functions, or otherwise for purposes of security, communicate to another person, make use of, or make a record of the following:
- (a) lawfully accessed information other than foreign intelligence information;
 - (aa) preservation notice information;
 - (b) stored communications warrant information.

Section 137

- (2) The Director-General of Security may, in connection with the performance by the Organisation of its functions, communicate foreign intelligence information to an ASIO employee or ASIO affiliate.
- (3) An ASIO employee or ASIO affiliate may, in connection with the performance by the Organisation of its functions, communicate foreign intelligence information to the Director-General of Security or to another ASIO employee or ASIO affiliate.
- (4) The Director-General of Security or an ASIO employee or ASIO affiliate may, in connection with the performance by the Organisation of its functions, make use of, or make a record of, foreign intelligence information.

137 Dealing in information obtained by Organisation

- (1) The Director-General of Security may, in accordance with subsection 18(3) or (4A), or subsection 19A(4) of the *Australian Security Intelligence Organisation Act 1979*, communicate the following to another person:
 - (a) lawfully accessed information;
 - (aa) preservation notice information;
 - (b) stored communications warrant information.
- (2) The communication may be made by the Director-General of Security personally or by a person authorised by the Director-General.
- (3) A person to whom foreign intelligence information has been communicated:
 - (a) in accordance with subsection (1); or
 - (b) in accordance with an approval given under this subsection;may:
 - (c) communicate that information to such persons, and in such manner, as are approved in writing by the Attorney-General; and

- (d) use that information for such purposes as are approved in writing by the Attorney-General; and
 - (e) make a record of that information.
- (4) An approval under subsection (3) is not a legislative instrument.

138 Employee of carrier may communicate information to criminal law-enforcement agency

- (1) An employee of a carrier may, for a purpose or purposes connected with the investigation by the Australian Communications and Media Authority of a serious contravention or with the performance of its functions relating to enforcement of the *Spam Act 2003*, and for no other purpose, communicate to an officer or staff member of the authority the following:
- (a) lawfully accessed information other than foreign intelligence information;
 - (aa) preservation notice information;
 - (b) stored communications warrant information.
- (2) An employee of a carrier may, for a purpose or purposes connected with the investigation by any other criminal law-enforcement agency of a serious contravention, and for no other purpose, communicate to an officer or staff member of the agency the following:
- (a) lawfully accessed information other than foreign intelligence information;
 - (aa) preservation notice information;
 - (b) stored communications warrant information.

139 Dealing for purposes of investigation etc.

- (1) An officer or staff member of a criminal law-enforcement agency or an eligible Commonwealth authority may, for one or more purposes referred to in subsection (2) or (4A), and for no other purpose (other than a purpose referred to in subsection 139A(2) or 139B(2), if applicable), communicate to another person, make use of, or make a record of the following:

Section 139

- (a) lawfully accessed information other than foreign intelligence information;
 - (aa) preservation notice information;
 - (b) stored communications warrant information.
- (2) In the case of information obtained by the agency other than through the execution of a warrant issued as a result of an international assistance application, the purposes are purposes connected with:
- (a) an investigation by the agency or by another criminal law-enforcement agency of a contravention to which subsection (3) applies; or
 - (b) the making by an authority, body or person of a decision whether or not to begin a proceeding to which subsection (4) applies; or
 - (c) a proceeding to which subsection (4) applies; or
 - (d) the keeping of records by the agency under Part 3-5; or
 - (e) an authorisation under any of the following provisions in respect of the information:
 - (i) subsection 13A(1) of the *Mutual Assistance in Criminal Matters Act 1987*;
 - (ii) section 69A of the *International Criminal Court Act 2002*;
 - (iii) section 25A of the *International War Crimes Tribunals Act 1995*.
- (3) A contravention to which this subsection applies is a contravention of a law of the Commonwealth, a State or a Territory that:
- (a) is a serious offence; or
 - (b) is an offence punishable:
 - (i) by imprisonment for a period, or a maximum period, of at least 12 months; or
 - (ii) if the offence is committed by an individual—by a fine, or a maximum fine, of at least 60 penalty units; or

- (iii) if the offence cannot be committed by an individual—
by a fine, or a maximum fine, of at least 300 penalty
units; or
- (c) could, if established, render the person committing the
contravention liable:
 - (i) if the contravention were committed by an individual—
to pay a pecuniary penalty of 60 penalty units or more,
or to pay an amount that is the monetary equivalent of
60 penalty units or more; or
 - (ii) if the contravention cannot be committed by an
individual—to pay a pecuniary penalty of 300 penalty
units or more, or to pay an amount that is the monetary
equivalent of 300 penalty units or more.
- (4) A proceeding to which this subsection applies is:
 - (a) a proceeding by way of a prosecution for an offence of a kind
referred to in paragraph (3)(a) or (b); or
 - (b) a proceeding for the confiscation or forfeiture of property, or
for the imposition of a pecuniary penalty, in connection with
the commission of such an offence; or
 - (ba) a proceeding under the *Spam Act 2003*; or
 - (c) a proceeding for the taking of evidence pursuant to section 43
of the *Extradition Act 1988*, in so far as the proceeding
relates to such an offence; or
 - (d) a proceeding for the extradition of a person from a State or a
Territory to another State or Territory, in so far as the
proceeding relates to such an offence; or
 - (e) a proceeding for recovery of a pecuniary penalty for a
contravention of a kind referred to in paragraph (3)(c); or
 - (f) a police disciplinary proceeding.
- (4A) In the case of information obtained by the agency through the
execution of a warrant issued as a result of an international
assistance application, the purposes are purposes connected with:
 - (a) providing the information to the entity to which the
application relates, or to an appropriate authority of that
entity; or

Section 139A

- (b) the keeping of records by the agency under Part 3-5.
- (5) To avoid doubt, a reference in subsection (3) to a number of penalty units in relation to a contravention of a law of a State or a Territory includes a reference to an amount of a fine or pecuniary penalty that is equivalent, under section 4AA of the *Crimes Act 1914*, to that number of penalty units.

139A Dealing for integrity purposes

- (1) An officer or staff member of a Commonwealth agency may, for one or more purposes referred to in subsection (2), and for no other purpose (other than a purpose referred to in subsection 139(2) or (4A) or 139B(2), if applicable), communicate to another person, make use of, or make a record of the following:
 - (a) lawfully accessed information other than foreign intelligence information;
 - (b) stored communications warrant information.
- (2) The purposes are:
 - (a) a permitted purpose mentioned in the table in section 6S in relation to the agency or another Commonwealth agency; or
 - (b) purposes connected with the keeping of records by the agency under Part 3-5.

139B Dealing for purposes relating to Part 5.3 orders

- (1) An officer or staff member of:
 - (a) the Australian Federal Police; or
 - (b) the Police Force of a State or Territory;may, for one or more purposes referred to in subsection (2), and for no other purpose (other than a purpose referred to in subsection 139(2) or (4A) or 139A(2), if applicable), communicate to another person, make use of, or make a record of lawfully accessed information other than foreign intelligence information.

- (2) The purposes are purposes connected with the performance of a function or duty, or the exercise of a power, by a person, court or other body under, or in relation to a matter arising under:
- (a) Division 104 (control orders) or Division 105A (post-sentence orders) of the *Criminal Code*; or
 - (b) a post-sentence detention law or a post-sentence supervision law.

140 Dealing with information if access suspected to be unlawful

- (1) A person may communicate information to the Minister, the Director of Public Prosecutions, the Commissioner of Police, the Integrity Commissioner or the Chief Executive Officer of the ACC if:
- (a) the information was obtained by accessing a stored communication; and
 - (b) the person suspects on reasonable grounds that the information may tend to establish that an offence of the following kind (a *suspected offence*) has been committed:
 - (i) an offence against subsection 108(1) constituted by the access, or by authorising, suffering or permitting, or doing an act or thing to enable, the access;
 - (ii) an offence against section 133 constituted by communicating to a person, making use of, making a record of, or giving in evidence in a proceeding, information obtained by the access;
 - (iii) an ancillary offence relating to an offence of a kind referred to in subparagraph (i) or (ii) of this paragraph.
- (2) A person to whom the information is communicated in accordance with subsection (1) may communicate to another person, make use of, or make a record of, some or all of the information for a purpose (or 2 or more purposes) connected with:
- (a) an investigation of a suspected offence; or
 - (b) the making by an authority, body or person of a decision whether or not to begin a proceeding by way of a prosecution for a suspected offence; or

Section 141

(c) a proceeding by way of a prosecution for a suspected offence;
and for no other purpose.

141 Making record for purpose of permitted communication

A person who is permitted by section 135, 137 or 138 or subsection 140(1) to communicate particular information to another person may:

- (a) make a record of the information, or
- (b) cause such a record to be made;

for the purpose of so communicating the information in accordance with that section or subsection.

142 Further dealing by recipient of certain information

A person to whom information has, in accordance with subsection 135(4), section 139, 139A or 139B, subsection 140(2) or this section, been communicated for a purpose, or for 2 or more purposes, may:

- (a) communicate that information to another person; or
- (b) make use of, or make a record of, that information;

for that purpose, or for one or more of those purposes, and for no other purpose.

142A Communicating information obtained as a result of an international assistance application

(1) If information is obtained through the execution of a warrant issued as a result of an international assistance application, a person may only communicate the information to the entity to which the application relates on the following conditions:

- (a) that the information will only be used for the purposes for which the entity requested the information;
- (b) that any document or other thing containing the information will be destroyed when it is no longer required for those purposes;

- (c) any other condition determined, in writing, by the Attorney-General.
- (2) Subsection (1) has effect despite subsection 139(4A) and section 142.
- (3) A determination under paragraph (1)(c) is not a legislative instrument.

143 Giving information in evidence in exempt proceeding

- (1) A person may give lawfully accessed information (other than foreign intelligence information) in evidence in an exempt proceeding.
- (2) For the purposes of applying subsection (1) in relation to information, the question whether or not a stored communication was accessed in contravention of subsection 108(1) may be determined on the balance of probabilities.
- (3) A person may give stored communications warrant information in evidence in an exempt proceeding.

144 Giving information in evidence if communication unlawfully accessed

- (1) A person may give, in evidence in an exempt proceeding, information obtained by accessing stored communications obtained in contravention of subsection 108(1) if:
 - (a) the access was purportedly under a stored communications warrant; and
 - (b) the court in which, or the tribunal, body, authority or person before which, the proceeding is held is satisfied that:
 - (i) but for an irregularity, the access would not have constituted a contravention of subsection 108(1); and
 - (ii) the irregularity is not a substantial defect or irregularity; and

Section 145

- (iii) in all the circumstances, the irregularity should be disregarded.
- (2) A reference in subsection (1) to an irregularity is a reference to a defect or irregularity:
 - (a) in, or in connection with the issue of, a document purporting to be a warrant; or
 - (b) in connection with the execution of a warrant, or the purported execution of a document purporting to be a warrant.

145 Evidence that has been given in exempt proceeding

If information is given in evidence in an exempt proceeding under section 143 or 144, that information, or any part of that information, may later be given in evidence in any proceeding.

Note: This section was inserted as a response to the decision of the Court of Appeal of New South Wales in *Wood v Beves* (1997) 92 A Crim R 209.

146 Giving information in evidence in civil proceedings for remedial relief

- (1) A person may give information obtained by accessing a stored communication in contravention of subsection 108(1) in evidence in a proceeding by way of an application under section 165 for remedial relief in respect of:
 - (a) the access; or
 - (b) the communication (in contravention of section 133) of information obtained by the access.
- (2) A person may give preservation notice information or stored communications warrant information in evidence in a proceeding by way of an application under section 165.

Division 3—Admissibility of evidence

147 Accessed material inadmissible except as provided

- (1) Neither information, nor a record, obtained by accessing a stored communication is admissible in evidence in a proceeding except in so far as section 143, 144, 145 or 146 permits a person to give in evidence in that proceeding information so obtained.
- (2) Subsection (1) of this section applies whether or not the stored communication was accessed in contravention of subsection 108(1).
- (3) However, for the purpose of determining the extent (if any) to which section 143, 144, 145 or 146 permits a person to give in evidence in a proceeding information obtained by the access:
 - (a) a person may communicate to another person, make use of, make a record of, or give in evidence in the last-mentioned proceeding, information so obtained; and
 - (b) information, or a record, so obtained is admissible in evidence in the last-mentioned proceeding.

148 Stored communications warrant information inadmissible except as provided

- (1) Stored communications warrant information is admissible in evidence in a proceeding only to the extent that section 143, 145 or 146 permits a person to give stored communications warrant information in evidence in that proceeding.
- (2) For the purpose of determining the extent (if any) to which section 143, 145 or 146 permits a person to give stored communications warrant information in evidence in a proceeding:
 - (a) a person may:
 - (i) communicate the information to another person; or
 - (ii) make use of the information; or
 - (iii) make a record of the information; or

Section 149

- (iv) give the information in evidence in the proceeding; and
- (b) the information is admissible in evidence in the proceeding.

149 Evidence that is otherwise inadmissible

This Part does not render:

- (a) information; or
- (b) any record that was obtained by accessing a stored communication (whether or not in contravention of subsection 108(1));

admissible in evidence in a proceeding to a greater extent than it would have been admissible in evidence in that proceeding if this Part had not been enacted.

Division 4—Destruction of records

150 Destruction of records

- (1) If:
 - (a) information, or a record, that was obtained by accessing a stored communication (whether or not in contravention of subsection 108(1)) is in a criminal law-enforcement agency's possession; and
 - (b) the chief officer of the agency is satisfied that the information or record is not likely to be required for a purpose referred to in subsection 139(2) or (4A), 139A(2) or 139B(2);the chief officer must cause the information or record to be destroyed forthwith.
- (2) The chief officer must, as soon as practicable, and in any event within 3 months, after each 30 June, give to the Minister a written report that sets out the extent to which information and records were destroyed in accordance with this section.

Part 3-5—Keeping and inspection of records

Division 1—Obligation to keep records

151 Obligation to keep records

- (1) The chief officer of a criminal law-enforcement agency must cause the following, or copies of the following, to be kept in the agency's records for the period specified in subsection (3):
 - (a) each preservation notice given by the agency, and documents or other materials that indicate whether the notice was properly given;
 - (b) each notice under subsection 107L(3) of the revocation of such a preservation notice, and documents or other materials that indicate whether the revocation was properly made;
 - (c) each stored communications warrant issued to the agency, and documents or other materials that indicate whether the warrant was properly applied for, including:
 - (i) a copy of each application for such a warrant; and
 - (ii) a copy of each affidavit supporting such an application; and
 - (iii) documents or other materials that indicate whether the applicant for such a warrant complied with the requirements of Division 1 of Part 3-3;
 - (d) each instrument revoking such a warrant under section 122, and documents or other materials that indicate whether the revocation was properly made;
 - (e) documents or other materials that indicate the persons approved under subsection 127(2), and the persons appointed under subsection 127(3) to be approving officers for the purposes of subsection 127(2);
 - (f) each authorisation by the chief officer under subsection 135(2);

- (g) each request for international assistance, being a request to which an international assistance application relates, and documents or other materials that indicate:
 - (i) whether the request was made lawfully; or
 - (ii) the offence in relation to which the request was made;
 - (h) documents or other materials that indicate whether the communication, use or recording of lawfully accessed information (other than foreign intelligence information, preservation notice information or stored communication warrant information) complied with the requirements of Division 2 of Part 3-4;
 - (i) documents indicating whether information or a record was destroyed in accordance with section 150;
 - (j) each evidentiary certificate issued under this Chapter;
 - (k) each report given to the Minister under Division 1 of Part 3-6;
 - (l) documents and other materials of a kind prescribed under subsection (2) of this section.
- (2) The Minister may, by legislative instrument, prescribe kinds of documents and other materials that the chief officer of a criminal law-enforcement agency must cause to be kept in the agency's records.
- (3) The period for which the chief officer of a criminal law-enforcement agency must cause a particular item to be kept in the agency's records under subsection (1) of this section is the period:
- (a) starting when the item came into existence; and
 - (b) ending:
 - (i) when 3 years have elapsed since the item came into existence; or
 - (ii) when the Ombudsman gives a report to the Minister under section 186J that is about records that include the item;
- whichever happens earlier.

**Division 3—Inspection of preservation notice records by
Inspector-General of Intelligence and Security**

**158A Functions of the Inspector-General of Intelligence and
Security**

- (1) Under the *Inspector-General of Intelligence and Security Act 1986*, the Inspector-General of Intelligence and Security has functions in relation to preservation notices given by the Organisation.
- (2) In particular, the Inspector-General of Intelligence and Security has the function of:
 - (a) inquiring into any matter that relates to compliance by the Organisation with this Act (see subparagraph 8(1)(a)(i) of that Act); and
 - (b) conducting such inspections of the Organisation as the Inspector-General considers appropriate for the purpose of giving effect to the objects of that Act (see section 9A of that Act).

Part 3-6—Reports about access to stored communications

Division 1—Reports to the Minister

159 Annual reports regarding applications and warrants under Part 3-3

- (1) The chief officer of a criminal law-enforcement agency must, as soon as practicable, and in any event within 3 months, after each 30 June, give to the Minister a written report that sets out such information as:
 - (a) Division 2 (other than section 163A) requires to be set out in the Minister's report under that Division relating to the year ending on that 30 June; and
 - (b) can be derived from the agency's records.
- (2) Section 34C of the *Acts Interpretation Act 1901* does not apply in relation to a report under this section.

160 Minister may seek further information from Commonwealth agency

- (1) The Minister may, by writing, request the chief officer of a criminal law-enforcement agency to give to the Minister in writing specified information that:
 - (a) the Minister needs in connection with preparing a report under Division 2; and
 - (b) is not contained in a report by the chief officer under section 159.
- (2) To the extent that it is practicable to do so, the chief officer must comply with the request.

Division 2—Reports by the Minister

161 Annual report by Minister about stored communications warrants

The Minister must, as soon as practicable after each 30 June, cause to be prepared a written report that relates to the year ending on that 30 June and complies with this Division.

161A Report to contain information about preservation notices

Domestic preservation notices

- (1) The report must set out, for each criminal law-enforcement agency:
 - (a) the relevant statistics about domestic preservation notices that were given by the agency during that year; and
 - (b) the relevant statistics about revocation notices given by the agency under section 107L during that year.

Foreign preservation notices

- (2) If the criminal law-enforcement agency is the Australian Federal Police, the report must also set out:
 - (a) the relevant statistics about foreign preservation notices that were given by the agency during that year; and
 - (b) the relevant statistics about revocation notices given by the agency under section 107R during that year.

162 Report to set out how many applications made and warrants issued

- (1) The report must set out, for each criminal law-enforcement agency:
 - (a) the relevant statistics about applications for stored communications warrants that the agency made during that year; and

- (b) the relevant statistics about telephone applications for stored communications warrants that the agency made during that year; and
 - (c) the relevant statistics about international assistance applications that the agency made during that year; and
 - (d) for each international offence for the agency—the offence (if any), under a law of the Commonwealth, a State or a Territory, that is of the same, or a substantially similar, nature to the international offence.
- (2) The report must set out:
- (a) the relevant statistics about applications for stored communications warrants that were made during that year; and
 - (b) the relevant statistics about telephone applications for stored communications warrants that were made during that year; and
 - (ba) the relevant statistics about international assistance applications that were made during that year; and
 - (c) the relevant statistics about renewal applications made during that year; and
 - (d) how many stored communications warrants issued on applications made during that year specified conditions or restrictions relating to access to stored communications under the warrants; and
 - (e) for each international offence for each enforcement agency—the offence (if any), under a law of the Commonwealth, a State or a Territory, that is of the same, or a substantially similar, nature to the international offence.
- (3) An **international offence**, for an enforcement agency, is:
- (a) an offence against a law of a foreign country; or
 - (b) a crime within the jurisdiction of the ICC; or
 - (c) a War Crimes Tribunal offence;
- in respect of which a stored communications warrant was issued as a result of an international assistance application made by the agency during the year.
-

Section 163

163 Report to contain information about effectiveness of warrants

The report must set out, for each criminal law-enforcement agency:

- (a) how many arrests were made during that year on the basis of information that was, or included, lawfully accessed information; and
- (b) how many proceedings ended during that year that were proceedings in which, according to the records of the agency, lawfully accessed information was given in evidence.

163A Report regarding international requests

The report must set out the number of occasions on which lawfully accessed information or stored communications warrant information was communicated under subsection 139(1) or section 142 to any of the following:

- (a) a foreign country;
- (b) the International Criminal Court;
- (c) a War Crimes Tribunal;

for a purpose connected with an authorisation referred to in paragraph 139(2)(e).

Division 3—Provisions about annual reports

164 Annual reports

- (1) The Minister must cause a copy of a report under Division 2 to be laid before each House of the Parliament within 15 sitting days of that House after the report is prepared.
- (2) A report under Division 2 must not be made in a manner that is likely to enable the identification of a person.
- (3) For the purposes of section 34C of the *Acts Interpretation Act 1901*, a report that Division 2 requires to be prepared as soon as practicable after 30 June in a calendar year is taken to be a periodic report:
 - (a) that this Act requires a person to give to the Minister; and
 - (b) that relates to the administration of Parts 3-3, 3-4 and 3-5 during the year ending on that 30 June.

Part 3-7—Civil remedies

165 Civil remedies—unlawful access or communication

When section applies

- (1) This section applies to an accessing of a stored communication if the access was in contravention of subsection 108(1).

Aggrieved person

- (2) For the purposes of this section, a person is an **aggrieved person** if, and only if:
- (a) the person was a party to the communication; or
 - (b) the communication was made on the person's behalf.

Access—civil court remedy

- (3) If a person (the **defendant**):
- (a) so accessed the communication; or
 - (b) did an act or thing referred to in subparagraph 108(1)(a)(ii) or (iii) in relation to the access;

the Federal Court of Australia or a court of a State or Territory may, on the application of an aggrieved person, grant the aggrieved person remedial relief in respect of the access by making such orders against the defendant as the court considers appropriate.

Note: Subparagraphs 108(1)(a)(ii) and (iii) deal with the authorisation or enabling of access etc.

Communication—civil court remedy

- (4) If:
- (a) information was obtained by accessing the communication; and
 - (b) a person (the **defendant**) communicated the information to another person in contravention of section 133;

the Federal Court of Australia or a court of a State or Territory may, on the application of an aggrieved person, grant the aggrieved person remedial relief in respect of the communication of the information by making such orders against the defendant as the court considers appropriate.

Access—criminal court remedy

- (5) If a court convicts a person (the ***defendant***) of an offence against subsection 108(1) constituted by:
- (a) the access; or
 - (b) the doing of an act or thing referred to in subparagraph 108(1)(a)(ii) or (iii) in relation to the access;
- the court may, on the application of an aggrieved person, grant the aggrieved person remedial relief in respect of the access by making such orders against the defendant as the court considers appropriate.

Note: Subparagraphs 108(1)(a)(ii) and (iii) deal with the authorisation or enabling of access etc.

Communication—criminal court remedy

- (6) If:
- (a) information was obtained by accessing the communication; and
 - (b) the information was communicated to a person in contravention of section 133; and
 - (c) a court convicts a person (in this subsection called the ***defendant***) of an offence against section 133 constituted by the communication of the information;
- the court may, on the application of an aggrieved person, grant the aggrieved person remedial relief in respect of the communication of the information by making such orders against the defendant as the court considers appropriate.

Section 165

Orders

- (7) Without limiting the orders that may be made under this section against a person (the *defendant*) in respect of a particular access to or a particular communication of information, a court may make an order of one or more of the following kinds:
- (a) an order declaring the access or communication, as the case requires, to have been unlawful;
 - (b) an order that the defendant pay to the aggrieved person such damages as the court considers appropriate;
 - (c) an order in the nature of an injunction (including a mandatory injunction);
 - (d) an order that the defendant pay to the aggrieved person an amount not exceeding the amount that, in the opinion of the court, represents the total gross income derived by the defendant as a result of the access or communication, as the case requires.

Terms etc. of orders

- (8) Without limiting the orders that may be made by a court under this section, an order may:
- (a) include such provisions as the court considers necessary for the purposes of the order; and
 - (b) be made either unconditionally or subject to such terms and conditions as the court determines.

Injunctive relief—variation etc.

- (9) A court may revoke or vary an order in the nature of an injunction made by the court under this section.

Punitive damages

- (10) A reference in paragraph (7)(b) to damages includes a reference to damages in the nature of punitive damages.

Minor irregularities in warrants etc.

- (11) Despite subsection (1) of this section, this section does not apply to an accessing that contravenes subsection 108(1) only because of a defect or irregularity (other than a substantial defect or irregularity):
- (a) in, or in connection with the issue of, a document purporting to be a warrant; or
 - (b) in connection with the execution of a warrant, or the purported execution of a document purporting to be a warrant.

166 Limitation periods etc.

Access—civil court remedy

- (1) An application under subsection 165(3) for the grant of remedial relief in respect of an access is to be made within 6 years after the access took place.

Communication—civil court remedy

- (2) An application under subsection 165(4) for the grant of remedial relief in respect of a communication of information is to be made within 6 years after the communication.

Criminal court remedies

- (3) An application under subsection 165(5) or (6) for the grant of remedial relief is not subject to any limitation period, but is to be made as soon as practicable after the conviction concerned.

167 No limitation on other liability

No limitation

- (1) This Part does not limit any liability (whether criminal or civil) that a person has under any other provision of this Act or under any other law.

Section 168

Remedial relief even if defendant convicted of offence

- (2) An application under subsection 165(3) or (4) may be made even if the defendant referred to in that subsection has been convicted of an offence under, or arising out of, this Act.

168 Concurrent operation of State and Territory laws

This Part is not intended to exclude or limit the operation of a law of a State or Territory that is capable of operating concurrently with this Part.

169 State or Territory courts—jurisdictional limits

This Part does not enable an inferior court of a State or Territory to grant remedial relief of a kind that the court is unable to grant under the law of that State or Territory.

170 Extended meaning of *conviction*—orders under section 19B of the *Crimes Act 1914*

A reference in this Part to the conviction of a person of an offence includes a reference to the making of an order under section 19B of the *Crimes Act 1914* in relation to a person in respect of an offence.

Note: Section 19B of the *Crimes Act 1914* empowers a court that has found a person to have committed an offence to take action without proceeding to record a conviction.

Chapter 4—Access to telecommunications data

Part 4-1—Permitted access to telecommunications data

Division 1—Outline of Part

171 Outline of Part

- (1) Divisions 3, 4 and 4A set out some circumstances when sections 276, 277 and 278 of the *Telecommunications Act 1997* do not prohibit a disclosure of information or a document.

Note 1: Division 3 covers the Organisation. Division 4 covers disclosures for the purposes of Australian enforcement agencies. Division 4A covers disclosures for the purposes of foreign law enforcement.

Note 2: Those Divisions do not permit the disclosure of the contents or substance of a communication: see Division 2.

- (2) Division 5 sets out some circumstances when sections 276, 277 and 278 of the *Telecommunications Act 1997* do not prohibit a use of information or a document.
- (3) Division 6 creates offences for certain disclosures and uses of information and documents.

Division 2—General provisions

172 No disclosure of the contents or substance of a communication

Divisions 3, 4 and 4A do not permit the disclosure of:

- (a) information that is the contents or substance of a communication; or
- (b) a document to the extent that the document contains the contents or substance of a communication.

173 Effect of Divisions 3 to 5

Nothing in Divisions 3 to 5 limits the generality of anything else in those Divisions or in Subdivision A of Division 3 of Part 13 of the *Telecommunications Act 1997*.

Division 3—The Organisation

174 Voluntary disclosure

- (1) Sections 276, 277 and 278 of the *Telecommunications Act 1997* do not prohibit a disclosure by a person (the **holder**) of information or a document to the Organisation if the disclosure is in connection with the performance by the Organisation of its functions.

Limitation

- (2) This section does not apply if the Director-General of Security, the Deputy Director-General of Security or any other ASIO employee or ASIO affiliate requests the holder to disclose the information or document.

Note: Sections 175 and 176 deal with the disclosure of information or a document in response to authorisations by the Organisation.

175 Authorisations for access to existing information or documents

- (1) Sections 276, 277 and 278 of the *Telecommunications Act 1997* do not prohibit a disclosure of information or a document if the information or document is covered by an authorisation in force under subsection (2).

Making of authorisation

- (2) The following persons (each of whom is an **eligible person**):
- (a) the Director-General of Security;
 - (b) the Deputy Director-General of Security;
 - (c) ASIO employee or ASIO affiliate covered by an approval in force under subsection (4);
- may authorise the disclosure of specified information or specified documents that came into existence before the time the person from whom the disclosure is sought receives notification of the authorisation.

Note: Section 184 deals with notification of authorisations.

Section 176

- (3) The eligible person must not make the authorisation unless he or she is satisfied that the disclosure would be in connection with the performance by the Organisation of its functions.

Approvals

- (4) The Director-General of Security may, by writing, approve ASIO employee or ASIO affiliate for the purposes of paragraph (2)(c).

176 Authorisations for access to prospective information or documents

- (1) Sections 276, 277 and 278 of the *Telecommunications Act 1997* do not prohibit a disclosure of information or a document if the information or document is covered by an authorisation in force under this section.

Prospective authorisation

- (2) The following persons (each of whom is an *eligible person*):

- (a) the Director-General of Security;
- (b) the Deputy Director-General of Security;
- (c) an ASIO employee or ASIO affiliate who holds, or is acting in, a position that is equivalent to, or that is higher than, an SES Band 2 position in the Department;

may authorise the disclosure of specified information or specified documents that come into existence during the period for which the authorisation is in force.

Authorisation for access to existing information or documents may also be sought

- (3) The eligible person may, in that authorisation, also authorise the disclosure of specified information or specified documents that came into existence before the time the authorisation comes into force.

Limits on making the authorisation

- (4) The eligible person must not make the authorisation unless he or she is satisfied that the disclosure would be in connection with the performance by the Organisation of its functions.

Period for which authorisation is in force

- (5) An authorisation under this section:
- (a) comes into force at the time the person from whom the disclosure is sought receives notification of the authorisation; and
 - (b) unless it is revoked earlier, ends at the time specified in the authorisation, which must be a time that:
 - (i) is no later than the end of the period of 90 days beginning on the day the authorisation is made; and
 - (ii) if the authorisation is made under a journalist information warrant—is no later than the end of the period specified under section 180N as the period for which the warrant is to remain in force.

Note: Section 184 deals with notification of authorisations.

Revoking the authorisation

- (6) An eligible person must revoke the authorisation if:
- (a) he or she is satisfied that the disclosure is no longer required; or
 - (b) in a case where the authorisation is made under a journalist information warrant:
 - (i) the warrant is revoked under subsection 180N(1); or
 - (ii) the Director-General of Security has informed the Attorney-General under section 180P that the Director-General is satisfied that the grounds on which the warrant was issued have ceased to exist.

Note: Section 184 deals with notification of authorisations.

Division 4—Enforcement agencies

176A Meaning of *enforcement agency*

- (1) Each of the following is an *enforcement agency*:
 - (a) subject to subsection 110A(7), a criminal law-enforcement agency;
 - (b) subject to subsection (7), an authority or body for which a declaration under subsection (3) is in force.

Note: See also section 110B (about declarations in relation to the Immigration and Border Protection Department).
- (2) The head of an authority or body may request the Minister to declare the authority or body to be an enforcement agency.
- (3) The Minister may, by legislative instrument, declare:
 - (a) an authority or body to be an enforcement agency; and
 - (b) persons specified, or of a kind specified, in the declaration to be officers of the enforcement agency for the purposes of this Act.
- (3A) The Minister may make the declaration whether or not the head of the authority or body has made a request under subsection (2).
- (3B) The Minister must not make the declaration unless the Minister is satisfied on reasonable grounds that the functions of the authority or body include:
 - (a) enforcement of the criminal law; or
 - (b) administering a law imposing a pecuniary penalty; or
 - (c) administering a law relating to the protection of the public revenue.
- (4) In considering whether to make the declaration, the Minister must have regard to:
 - (b) whether the making of authorisations under section 178 or 179 would be reasonably likely to assist the authority or body

- in performing the functions referred to in subsection (3B);
and
- (c) whether the authority or body:
 - (i) is required to comply with the Australian Privacy Principles; or
 - (ii) is required to comply with a binding scheme that provides protection of personal information that meets the requirements of subsection (4A); or
 - (iii) has agreed in writing to comply with a scheme providing such protection of personal information, in relation to personal information disclosed to it under Chapter 4, if the declaration is made; and
 - (d) whether the authority or body proposes to adopt processes and practices that would ensure its compliance with the obligations of an enforcement agency under Chapter 4; and
 - (e) whether the Minister considers that the declaration would be in the public interest; and
 - (f) any other matter that the Minister considers relevant.
- (4A) For the purposes of subparagraphs (4)(c)(ii) and (iii), the protection of personal information provided by the scheme must:
- (a) be comparable to the protection provided by the Australian Privacy Principles; and
 - (b) include a mechanism for monitoring the authority's or body's compliance with the scheme; and
 - (c) include a mechanism that enables an individual to seek recourse if his or her personal information is mishandled.
- (5) In considering whether to make the declaration, the Minister may consult such persons or bodies as the Minister thinks fit. In particular, the Minister may consult the Privacy Commissioner and the Ombudsman.
- (6) The declaration may be subject to conditions.
- (7) Without limiting subsection (6), a condition may provide that the authority or body is not to exercise a power conferred on an enforcement agency by or under a specified provision in Chapter 4.
-

Section 177

The authority or body is taken, for the purposes of this Act, not to be an enforcement agency for the purposes of that provision.

- (8) The Minister may, by legislative instrument, revoke a declaration under subsection (3) relating to an authority or body if the Minister is no longer satisfied that the circumstances justify the declaration remaining in force.
- (9) The revocation under subsection (8) of a declaration relating to an authority or body does not affect the validity of an authorisation, made by an authorised officer of the authority or body under this Division, that was in force immediately before the revocation took effect.
- (10) A declaration under subsection (3):
 - (a) comes into force when it is made, or on such later day as is specified in the declaration; and
 - (b) ceases to be in force at the end of the period of 40 sitting days of a House of the Parliament after the declaration comes into force.
- (11) If a Bill is introduced into either House of the Parliament that includes an amendment of subsection (1), the Minister:
 - (a) must refer the amendment to the Parliamentary Joint Committee on Intelligence and Security for review; and
 - (b) must not in that referral specify, as the period within which the Committee is to report on its review, a period that will end earlier than 15 sitting days of a House of the Parliament after the introduction of the Bill.

177 Voluntary disclosure

Enforcement of the criminal law

- (1) Sections 276, 277 and 278 of the *Telecommunications Act 1997* do not prevent a disclosure by a person (the **holder**) of information or a document to an enforcement agency if the disclosure is reasonably necessary for the enforcement of the criminal law.

Enforcement of a law imposing a pecuniary penalty or protection of the public revenue

- (2) Sections 276 and 277 of the *Telecommunications Act 1997* do not prevent a disclosure by a person (the **holder**) of information or a document to an enforcement agency if the disclosure is reasonably necessary for the enforcement of a law imposing a pecuniary penalty or for the protection of the public revenue.

Limitation

- (3) This section does not apply if a relevant staff member of an enforcement agency requests the holder to disclose the information or document.

Note: Sections 178 to 180 deal with the disclosure of information or a document in response to authorisations by an authorised officer of an enforcement agency.

178 Authorisations for access to existing information or documents—enforcement of the criminal law

- (1) Sections 276, 277 and 278 of the *Telecommunications Act 1997* do not prevent a disclosure of information or a document if the information or document is covered by an authorisation in force under subsection (2).
- (2) An authorised officer of an enforcement agency may authorise the disclosure of specified information or specified documents that came into existence before the time the person from whom the disclosure is sought receives notification of the authorisation.

Note: Section 184 deals with notification of authorisations.

- (3) The authorised officer must not make the authorisation unless he or she is satisfied that the disclosure is reasonably necessary for the enforcement of the criminal law.

Section 178A

178A Authorisations for access to existing information or documents—locating missing persons

- (1) Sections 276, 277 and 278 of the *Telecommunications Act 1997* do not prevent a disclosure of information or a document if the information or document is covered by an authorisation in force under subsection (2).
- (2) An authorised officer of the Australian Federal Police, or a Police Force of a State, may authorise the disclosure of specified information or specified documents that came into existence before the time the person from whom the disclosure is sought receives notification of the authorisation.

Note: Section 184 deals with notification of authorisations.

- (3) The authorised officer must not make the authorisation unless he or she is satisfied that the disclosure is reasonably necessary for the purposes of finding a person who the Australian Federal Police, or a Police Force of a State, has been notified is missing.

179 Authorisations for access to existing information or documents—enforcement of a law imposing a pecuniary penalty or protection of the public revenue

- (1) Sections 276 and 277 of the *Telecommunications Act 1997* do not prevent a disclosure of information or a document if the information or document is covered by an authorisation in force under subsection (2).
- (2) An authorised officer of an enforcement agency may authorise the disclosure of specified information or specified documents that came into existence before the time the person from whom the disclosure is sought receives notification of the authorisation.

Note: Section 184 deals with notification of authorisations.

- (3) The authorised officer must not make the authorisation unless he or she is satisfied that the disclosure is reasonably necessary for the enforcement of a law imposing a pecuniary penalty or for the protection of the public revenue.

180 Authorisations for access to prospective information or documents

- (1) Sections 276, 277 and 278 of the *Telecommunications Act 1997* do not prevent a disclosure of information or a document if the information or document is covered by an authorisation in force under this section.

Prospective authorisation

- (2) An authorised officer of a criminal law-enforcement agency may authorise the disclosure of specified information or specified documents that come into existence during the period for which the authorisation is in force.

Authorisation for access to existing information or documents may also be sought

- (3) The authorised officer may, in that authorisation, also authorise the disclosure of specified information or specified documents that came into existence before the time the authorisation comes into force.

Limits on making the authorisation

- (4) The authorised officer must not make the authorisation unless he or she is satisfied that the disclosure is reasonably necessary for the investigation of:
- (a) a serious offence; or
 - (b) an offence against a law of the Commonwealth, a State or a Territory that is punishable by imprisonment for at least 3 years.

Period for which authorisation is in force

- (6) An authorisation under this section:
- (a) comes into force at the time the person from whom the disclosure is sought receives notification of the authorisation; and

Section 180

- (b) unless it is revoked earlier, ends at the time specified in the authorisation, which must be a time that:
 - (i) is no later than the end of the period of 45 days beginning on the day the authorisation is made; and
 - (ii) if the authorisation is made under a journalist information warrant—is no later than the end of the period specified under subsection 180U(3) as the period for which the warrant is to remain in force.

Note: Section 184 deals with notification of authorisations.

Revoking the authorisation

- (7) An authorised officer of the criminal law-enforcement agency must revoke the authorisation if:
 - (a) he or she is satisfied that the disclosure is no longer required; or
 - (b) in a case where the authorisation is made under a journalist information warrant—the warrant is revoked under subsection 180W(1).

Note: Section 184 deals with notification of authorisations.

Division 4A—Foreign law enforcement

Subdivision A—Primary disclosures

180A Authorisations for access to existing information or documents—enforcing foreign or international laws

Disclosure to the Australian Federal Police

- (1) Sections 276, 277 and 278 of the *Telecommunications Act 1997* do not prevent a disclosure of information or a document if the information or document is covered by an authorisation in force under subsection (2).
- (2) An authorised officer of the Australian Federal Police may authorise the disclosure of specified information or specified documents that came into existence before the time the person from whom the disclosure is sought receives notification of the authorisation.

Note: Section 184 deals with notification of authorisations.
- (3) The authorised officer must not make the authorisation unless he or she is satisfied that the disclosure is reasonably necessary for:
 - (a) the enforcement of the criminal law of a foreign country; or
 - (b) an investigation or prosecution of a crime within the jurisdiction of the ICC; or
 - (c) an investigation or prosecution of a War Crimes Tribunal offence.

Disclosure to a foreign law enforcement agency

- (4) If specified information or specified documents are disclosed because of an authorisation given under subsection (2), an authorised officer of the Australian Federal Police may authorise the disclosure of the information or documents so disclosed to a foreign law enforcement agency.

Section 180B

- (5) The authorised officer must not make the authorisation unless he or she is satisfied that the disclosure is appropriate in all the circumstances and that the disclosure is reasonably necessary for:
- (a) the enforcement of the criminal law of a foreign country; or
 - (b) an investigation or prosecution of a crime within the jurisdiction of the ICC; or
 - (c) an investigation or prosecution of a War Crimes Tribunal offence.

180B Authorisations for access to prospective information or documents—enforcing international laws

Disclosure to the Australian Federal Police

- (1) Sections 276, 277 and 278 of the *Telecommunications Act 1997* do not prevent a disclosure of information or a document if the information or document is covered by an authorisation in force under subsection (2) of this section.

Prospective authorisation

- (2) An authorised officer of the Australian Federal Police may authorise the disclosure of specified information or specified documents that come into existence during the period for which the authorisation is in force.
- (3) The authorised officer must not make the authorisation unless:
- (a) the Attorney-General has authorised the making of the authorisation under a provision mentioned in an item of the following table; and
 - (b) the authorised officer is satisfied that:
 - (i) the disclosure is reasonably necessary for an investigation or proceeding referred to in that table item; and
 - (ii) the disclosure is appropriate in all the circumstances.

Authorising access to prospective information or documents

Item	For Attorney-General authorisations under:	the investigation or proceeding is:
1	section 15D of the <i>Mutual Assistance in Criminal Matters Act 1987</i>	an investigation or proceeding relating to an offence against the law of a foreign country that: (a) is punishable by imprisonment for 3 years or more, imprisonment for life or the death penalty; or (b) involves an act or omission that, if it had occurred in Australia, would be a serious offence
2	section 78B of the <i>International Criminal Court Act 2002</i>	an investigation or proceeding relating to a crime within the jurisdiction of the ICC
3	section 34B of the <i>International War Crimes Tribunals Act 1995</i>	an investigation or proceeding relating to a War Crimes Tribunal offence

- (4) An authorised officer of the Australian Federal Police must revoke the authorisation if he or she is satisfied that the disclosure is no longer required.

Note: Section 184 deals with notification of revocations.

- (5) An authorisation under subsection (2):
- (a) comes into force at the time the person from whom the disclosure is sought receives notification of the authorisation; and
 - (b) ceases to be in force at the time specified in the authorisation, which must not be more than 21 days after the day the authorisation is made, or that period as extended under subsection (6), unless it is revoked earlier.

Note: Section 184 deals with notification of authorisations.

Extension of prospective authorisation

- (6) The period for which an authorisation under subsection (2) is in force may be extended once only, by an authorised officer of the

Section 180C

Australian Federal Police, if the authorised officer is satisfied that the extension is:

- (a) reasonably necessary for an investigation or proceeding of a kind referred to in the relevant table item in subsection (3); and
 - (b) appropriate in all the circumstances.
- (7) An extension under subsection (6) must not be for more than 21 days from the day of the extension.

Disclosure to a foreign law enforcement agency

- (8) If specified information or specified documents are disclosed because of an authorisation given under subsection (2), an authorised officer of the Australian Federal Police may authorise the disclosure of the information or documents so disclosed to a foreign law enforcement agency if the authorised officer is satisfied that the disclosure is:
- (a) reasonably necessary for an investigation or proceeding of a kind referred to in the relevant table item in subsection (3); and
 - (b) appropriate in all the circumstances.
- (9) An authorised officer must not make more than one authorisation a day under subsection (8).

Subdivision B—Secondary disclosures

**180C Authorisations to disclose information or documents—
enforcing foreign or international laws**

- (1) If specified information or specified documents are disclosed because of an authorisation given under Division 4, other than because of an authorisation under section 178A (missing persons), an authorised officer of the Australian Federal Police may authorise the disclosure of the information or documents so disclosed to a foreign law enforcement agency.

- (2) The authorised officer must not make the authorisation unless he or she is satisfied that the disclosure is appropriate in all the circumstances and that the disclosure is reasonably necessary for:
- (a) the enforcement of the criminal law of a foreign country; or
 - (b) an investigation or prosecution of a crime within the jurisdiction of the ICC; or
 - (c) an investigation or prosecution of a War Crimes Tribunal offence.

**180D Authorisations to disclose information or documents—
enforcement of the criminal law**

- (1) If specified information or specified documents are disclosed because of an authorisation given under this Division, an authorised officer of the Australian Federal Police may authorise the following:
- (a) the disclosure of the information or documents to the Organisation or an enforcement agency;
 - (b) the use of the information or documents by the Australian Federal Police.
- (2) The authorised officer must not make the authorisation unless he or she is satisfied that:
- (a) in the case of a disclosure to the Organisation—the disclosure is reasonably necessary for the performance by the Organisation of its functions; and
 - (b) in the case of a disclosure to an enforcement agency—the disclosure is reasonably necessary:
 - (i) for the enforcement of the criminal law; or
 - (ia) for the purposes of Division 105A of the *Criminal Code* (post-sentence orders); or
 - (ii) for the enforcement of a law imposing a pecuniary penalty; or
 - (iii) for the protection of the public revenue; and
 - (c) in the case of a use by the Australian Federal Police—the use is reasonably necessary:

Section 180E

- (i) for the enforcement of the criminal law; or
- (ia) for the purposes of Division 105A of the *Criminal Code* (post-sentence orders); or
- (ii) for the enforcement of a law imposing a pecuniary penalty; or
- (iii) for the protection of the public revenue; and
- (d) in any case—the disclosure or use is appropriate in all the circumstances.

Subdivision C—Conditions of disclosure to foreign law enforcement agencies

180E Disclosing information etc. to foreign countries or foreign law enforcement agencies

- (1) A person must not disclose information or a document in accordance with an authorisation under section 180A, 180B or 180C to a foreign country or foreign law enforcement agency unless the disclosure is subject to the following conditions:
 - (a) that the information will only be used for the purposes for which the foreign country or foreign law enforcement agency requested the information;
 - (b) that any document or other thing containing the information will be destroyed when it is no longer required for those purposes;
 - (c) in the case of information or a document disclosed under section 180B—any other condition determined, in writing, by the Attorney-General.
- (2) A determination made under paragraph (1)(c) is not a legislative instrument.

Division 4B—Privacy to be considered when making authorisations

180F Authorised officers to consider privacy

Before making an authorisation under Division 4 or 4A in relation to the disclosure or use of information or documents, the authorised officer considering making the authorisation must be satisfied on reasonable grounds that any interference with the privacy of any person or persons that may result from the disclosure or use is justifiable and proportionate, having regard to the following matters:

- (aa) the gravity of any conduct in relation to which the authorisation is sought, including:
 - (i) the seriousness of any offence in relation to which the authorisation is sought; and
 - (ii) the seriousness of any pecuniary penalty in relation to which the authorisation is sought; and
 - (iii) the seriousness of any protection of the public revenue in relation to which the authorisation is sought; and
 - (iv) whether the authorisation is sought for the purposes of finding a missing person;
- (a) the likely relevance and usefulness of the information or documents;
- (b) the reason why the disclosure or use concerned is proposed to be authorised.

Division 4C—Journalist information warrants

Subdivision A—The requirement for journalist information warrants

180G The Organisation

- (1) An eligible person (within the meaning of subsection 175(2) or 176(2), as the case requires) must not make an authorisation under Division 3 that would authorise the disclosure of information or documents relating to a particular person if:
 - (a) the eligible person knows or reasonably believes that particular person to be:
 - (i) a person who is working in a professional capacity as a journalist; or
 - (ii) an employer of such a person; and
 - (b) a purpose of making the authorisation would be to identify another person whom the eligible person knows or reasonably believes to be a source;unless a journalist information warrant is in force in relation to that particular person.
- (2) Nothing in this section affects by implication the kind of person in relation to whom a warrant (other than a journalist information warrant) may be issued under this Act.

180H Enforcement agencies

- (1) An authorised officer of an enforcement agency must not make an authorisation under section 178, 178A, 179 or 180 that would authorise the disclosure of information or documents relating to a particular person if:
 - (a) the authorised officer knows or reasonably believes that particular person to be:
 - (i) a person who is working in a professional capacity as a journalist; or

- (ii) an employer of such a person; and
 - (b) a purpose of making the authorisation would be to identify another person whom the authorised officer knows or reasonably believes to be a source;unless a journalist information warrant is in force, in relation to that particular person, under which authorised officers of the agency may make authorisations under that section.
- (2) An authorised officer of the Australian Federal Police must not make an authorisation under Division 4A that would authorise the disclosure of information or documents relating to a particular person if:
 - (a) the authorised officer knows or reasonably believes that particular person to be:
 - (i) a person who is working in a professional capacity as a journalist; or
 - (ii) an employer of such a person; and
 - (b) a purpose of making the authorisation would be to identify another person whom the authorised officer knows or reasonably believes to be a source.
- (3) Nothing in this section affects by implication the kind of person in relation to whom a warrant (other than a journalist information warrant) may be issued under this Act.

Subdivision B—Issuing journalist information warrants to the Organisation

180J Requesting a journalist information warrant

- (1) The Director-General of Security may request the Attorney-General to issue a journalist information warrant in relation to a particular person.
- (2) The request must specify the facts and other grounds on which the Director-General considers it necessary that the warrant be issued.

Section 180K

180K Further information

- (1) The Attorney-General may require the Director-General of Security to give to the Attorney-General, within the period specified in the requirement, further information in connection with a request under this Subdivision.
- (2) If the Director-General breaches the requirement, the Attorney-General may:
 - (a) refuse to consider the request; or
 - (b) refuse to take any action, or any further action, in relation to the request.

180L Issuing a journalist information warrant

- (1) After considering a request under section 180J, the Attorney-General must:
 - (a) issue a journalist information warrant that authorises the making of authorisations under Division 3 in relation to the particular person to which the request relates; or
 - (b) refuse to issue a journalist information warrant.
- (2) The Attorney-General must not issue a journalist information warrant unless the Attorney-General is satisfied that:
 - (a) the Organisation's functions would extend to the making of authorisations under Division 3 in relation to the particular person; and
 - (b) the public interest in issuing the warrant outweighs the public interest in protecting the confidentiality of the identity of the source in connection with whom authorisations would be made under the authority of the warrant, having regard to:
 - (i) the extent to which the privacy of any person or persons would be likely to be interfered with by the disclosure of information or documents under authorisations that are likely to be made under the authority of the warrant; and
 - (ii) the gravity of the matter in relation to which the warrant is sought; and

- (iii) the extent to which that information or those documents would be likely to assist in the performance of the Organisation's functions; and
 - (iv) whether reasonable attempts have been made to obtain the information or documents by other means; and
 - (v) any submissions made by a Public Interest Advocate under section 180X; and
 - (vi) any other matters the Attorney-General considers relevant.
- (3) A journalist information warrant issued under this section may specify conditions or restrictions relating to making authorisations under the authority of the warrant.

180M Issuing a journalist information warrant in an emergency

- (1) The Director-General of Security may issue a journalist information warrant in relation to a particular person if:
- (a) a request under section 180J has been made for the issue of a journalist information warrant in relation to the particular person; and
 - (b) the Attorney-General has not, to the knowledge of the Director-General, made a decision under section 180L in relation to the request; and
 - (c) within the preceding period of 3 months:
 - (i) the Attorney-General has not refused to issue a journalist information warrant in relation to the particular person; and
 - (ii) the Director-General has not issued such a journalist information warrant; and
 - (d) the Director-General is satisfied that, security will be, or is likely to be, seriously prejudiced if the access to which the request relates does not begin before a journalist information warrant can be issued and made available by the Attorney-General; and

Section 180M

- (e) either:
 - (i) the issuing of the warrant is authorised under subsection (3); or
 - (ii) the Director-General is satisfied that none of the Ministers specified in subsection (4) is readily available or contactable.
- (2) The Director-General must not issue a journalist information warrant unless the Director-General is satisfied as to the matters set out in paragraphs 180L(2)(a) and (b).

Authorisation to issue a warrant under this section

- (3) A Minister specified in subsection (4) may, if he or she is satisfied as to the matters set out in paragraphs 180L(2)(a) and (b), orally give an authorisation under this subsection for the Director-General to issue the warrant under this section.
- (4) The Ministers who may orally give an authorisation are:
 - (a) the Attorney-General; or
 - (b) if the Director-General is satisfied that the Attorney-General is not readily available or contactable—any of the following Ministers:
 - (i) the Prime Minister;
 - (ia) the most senior Minister administering this Act;
 - (ii) the Defence Minister;
 - (iii) the Foreign Affairs Minister.
- (5) The authorisation may specify conditions or restrictions relating to issuing the warrant.
- (6) The Director-General must ensure that a written record of an authorisation given under subsection (3) is made as soon as practicable (but no later than 48 hours) after the authorisation is given.

Duration of a warrant under this section

- (7) A journalist information warrant under this section must specify the period (not exceeding 48 hours) for which it is to remain in force. The Attorney-General may revoke the warrant at any time before the end of the specified period.

Copies of warrant and other documents

- (8) Immediately after issuing a journalist information warrant under this section, the Director-General must give the Attorney-General:
- (a) a copy of the warrant; and
 - (b) a statement of the grounds on which the warrant was issued; and
 - (c) either:
 - (i) a copy of the record made under subsection (6); or
 - (ii) if the Director-General was satisfied as mentioned in subparagraph (1)(e)(ii)—a summary of the facts of the case justifying issuing the warrant.
- (9) Within 3 business days after issuing a journalist information warrant under this section, the Director-General must give the Inspector-General of Intelligence and Security:
- (a) a copy of the warrant; and
 - (b) either:
 - (i) a copy of the record made under subsection (6); or
 - (ii) if the Director-General was satisfied as mentioned in subparagraph (1)(e)(ii)—a summary of the facts of the case justifying issuing the warrant.
- (10) Subsection (9) has effect despite subsection 185D(1).

180N Duration of a journalist information warrant

A journalist information warrant issued under section 180L must specify the period (not exceeding 6 months) for which it is to remain in force. The Attorney-General may revoke the warrant at any time before the end of the specified period.

Section 180P

180P Discontinuance of authorisations before expiry of a journalist information warrant

If, before a journalist information warrant issued under this Subdivision ceases to be in force, the Director-General of Security is satisfied that the grounds on which the warrant was issued have ceased to exist, he or she must:

- (a) forthwith inform the Attorney-General accordingly; and
- (b) takes such steps as are necessary to ensure that the making of authorisations under the authority of the warrant is discontinued.

Subdivision C—Issuing journalist information warrants to enforcement agencies

180Q Enforcement agency may apply for a journalist information warrant

- (1) An enforcement agency may apply to a Part 4-1 issuing authority for a journalist information warrant in relation to a particular person.
- (2) The application must be made on the agency's behalf by:
 - (a) if the agency is referred to in subsection 39(2)—a person referred to in that subsection in relation to that agency; or
 - (b) otherwise:
 - (i) the chief officer of the agency; or
 - (ii) an officer of the agency (by whatever name called) who holds, or is acting in, an office or position in the agency nominated under subsection (3).
- (3) The chief officer of the agency may, in writing, nominate for the purposes of subparagraph (2)(b)(ii) an office or position in the agency that is involved in the management of the agency.
- (4) A nomination under subsection (3) is not a legislative instrument.
- (5) The application may be made in writing or in any other form.

Note: The *Electronic Transactions Act 1999* deals with giving information in writing by means of an electronic communication.

180R Further information

- (1) The Part 4-1 issuing authority may require:
 - (a) in any case—the chief officer of the agency; or
 - (b) if the application is made, on the agency’s behalf, by a person other than the chief officer—that other person;to give to the Part 4-1 issuing authority, within the period and in the form specified in the requirement, further information in connection with the application.
- (2) If the chief officer or other person breaches the requirement, the Part 4-1 issuing authority may:
 - (a) refuse to consider the application; or
 - (b) refuse to take any action, or any further action, in relation to the application.

180S Oaths and affirmations

- (1) Information given to the Part 4-1 issuing authority in connection with the application must be verified on oath or affirmation.
- (2) For the purposes of this section, the Part 4-1 issuing authority may:
 - (a) administer an oath or affirmation; or
 - (b) authorise another person to administer an oath or affirmation.The oath or affirmation may be administered in person, or by telephone, video call, video link or audio link.

180T Issuing a journalist information warrant

- (1) After considering an application under section 180Q, the Part 4-1 issuing authority must:
 - (a) issue a journalist information warrant that authorises the making of authorisations under one or more of sections 178, 178A, 179 and 180 in relation to the particular person to which the application relates; or

Section 180T

- (b) refuse to issue a journalist information warrant.
- (2) The Part 4-1 issuing authority must not issue a journalist information warrant unless the Part 4-1 issuing authority is satisfied that:
 - (a) the warrant is reasonably necessary for whichever of the following purposes are applicable:
 - (i) if the warrant would authorise the making of authorisations under section 178—for the enforcement of the criminal law;
 - (ii) if the warrant would authorise the making of authorisations under section 178A—finding a person who the Australian Federal Police, or a Police Force of a State, has been notified is missing;
 - (iii) if the warrant would authorise the making of authorisations under section 179—the enforcement of a law imposing a pecuniary penalty or for the protection of the public revenue;
 - (iv) if the warrant would authorise the making of authorisations under section 180—the investigation of an offence of a kind referred to in subsection 180(4); and
 - (b) the public interest in issuing the warrant outweighs the public interest in protecting the confidentiality of the identity of the source in connection with whom authorisations would be made under the authority of the warrant, having regard to:
 - (i) the extent to which the privacy of any person or persons would be likely to be interfered with by the disclosure of information or documents under authorisations that are likely to be made under the authority of the warrant; and
 - (ii) the gravity of the matter in relation to which the warrant is sought; and
 - (iii) the extent to which that information or those documents would be likely to assist in relation to that matter; and
 - (iv) whether reasonable attempts have been made to obtain the information or documents by other means; and

- (v) any submissions made by a Public Interest Advocate under section 180X; and
- (vi) any other matters the Part 4-1 issuing authority considers relevant.

180U Form and content of a journalist information warrant

- (1) A journalist information warrant issued under this Subdivision must be in accordance with the prescribed form and must be signed by the Part 4-1 issuing authority who issues it.
- (2) A journalist information warrant issued under this Subdivision may specify conditions or restrictions relating to making authorisations under the authority of the warrant.
- (3) A journalist information warrant issued under this Subdivision must specify, as the period for which it is to be in force, a period of up to 90 days.
- (4) A Part 4-1 issuing authority must not vary a journalist information warrant issued under this Subdivision by extending the period for which it is to be in force.
- (5) Neither of subsections (3) and (4) prevents the issue of a further warrant under this Act in relation to a person, in relation to which a warrant under this Act has, or warrants under this Act have, previously been issued.

180V Entry into force of a journalist information warrant

A journalist information warrant issued under this Subdivision comes into force when it is issued.

180W Revocation of a journalist information warrant by chief officer

- (1) The chief officer of an enforcement agency:

Section 180X

- (a) may, at any time, by signed writing, revoke a journalist information warrant issued under this Subdivision to the agency; and
 - (b) must do so, if he or she is satisfied that the grounds on which the warrant was issued to the agency have ceased to exist.
- (2) The chief officer of an enforcement agency may delegate his or her power under paragraph (1)(a) to a certifying officer of the agency.

Subdivision D—Miscellaneous

180X Public Interest Advocates

- (1) The Prime Minister shall declare, in writing, one or more persons to be Public Interest Advocates.
- (2) A Public Interest Advocate may make submissions:
 - (a) to the Attorney-General about matters relevant to:
 - (i) a decision to issue, or refuse to issue, a journalist information warrant under section 180L; or
 - (ii) a decision about the conditions or restrictions (if any) that are to be specified in such a warrant; or
 - (b) to a Part 4-1 issuing authority about matters relevant to:
 - (i) a decision to issue, or refuse to issue, the warrant under section 180T; or
 - (ii) a decision about the conditions or restrictions (if any) that are to be specified in such a warrant.
- (3) The regulations may prescribe matters relating to the performance of the role of a Public Interest Advocate.
- (4) A declaration under subsection (1) is not a legislative instrument.

**Division 5—Uses of telecommunications data connected
with provision of access**

**181 Uses of telecommunications data connected with provision of
access**

Section 276, 277 or 278 of the *Telecommunications Act 1997* does not prohibit a use by a person of information or a document if:

- (a) the use is made for the purposes of, or in connection with, a disclosure of the information or document by the person; and
- (b) because of Division 3, 4 or 4A of this Part, the disclosure is not prohibited by that section.

Division 6—Disclosure/use offences

181A Disclosure/use offences: authorisations under Division 3

Disclosures

- (1) A person commits an offence if:
- (a) the person discloses information; and
 - (b) the information is about any of the following:
 - (i) whether an authorisation under Division 3 has been, or is being, sought;
 - (ii) the making of such an authorisation;
 - (iii) the existence or non-existence of such an authorisation;
 - (iv) the revocation of such an authorisation;
 - (v) the notification of such a revocation.

Penalty: Imprisonment for 2 years.

- (2) A person commits an offence if:
- (a) the person discloses a document; and
 - (b) the document consists (wholly or partly) of any of the following:
 - (i) an authorisation under Division 3;
 - (ii) the revocation of such an authorisation;
 - (iii) the notification of such a revocation.

Penalty: Imprisonment for 2 years.

- (3) Paragraphs (1)(a) and (2)(a) do not apply to a disclosure of information or a document if:
- (a) the disclosure is for the purposes of the authorisation, revocation or notification concerned; or
 - (b) the disclosure is reasonably necessary:
 - (i) to enable the Organisation to perform its functions; or
 - (ia) to enable a person to comply with his or her obligations under section 185D or 185E; or

- (ii) to enforce the criminal law; or
- (iii) to enforce a law imposing a pecuniary penalty; or
- (iv) to protect the public revenue; or
- (c) the disclosure is:
 - (i) to an IGIS official for the purpose of the Inspector-General of Intelligence and Security exercising powers, or performing functions or duties, under the *Inspector-General of Intelligence and Security Act 1986*; or
 - (ii) by an IGIS official in connection with the IGIS official exercising powers, or performing functions or duties, under that Act.

Note: A defendant bears an evidential burden in relation to the matter in subsection (3) (see subsection 13.3(3) of the *Criminal Code*).

Uses

- (4) A person commits an offence if:
 - (a) the person uses information; and
 - (b) the information is about any of the following:
 - (i) whether an authorisation under Division 3 has been, or is being, sought;
 - (ii) the making of such an authorisation;
 - (iii) the existence or non-existence of such an authorisation;
 - (iv) the revocation of such an authorisation;
 - (v) the notification of such a revocation.

Penalty: Imprisonment for 2 years.

- (5) A person commits an offence if:
 - (a) the person uses a document; and
 - (b) the document consists (wholly or partly) of any of the following:
 - (i) an authorisation under Division 3;
 - (ii) the revocation of such an authorisation;
 - (iii) the notification of such a revocation.

Section 181B

Penalty: Imprisonment for 2 years.

- (6) Paragraphs (4)(a) and (5)(a) do not apply to a use of information or a document if:
- (a) the use is for the purposes of the authorisation, revocation or notification concerned; or
 - (b) the use is reasonably necessary:
 - (i) to enable the Organisation to perform its functions; or
 - (ia) to enable a person to comply with his or her obligations under section 185D or 185E; or
 - (ii) to enforce the criminal law; or
 - (iii) to enforce a law imposing a pecuniary penalty; or
 - (iv) to protect the public revenue; or
 - (c) the use is by an IGIS official in connection with the IGIS official exercising powers, or performing functions or duties, under the *Inspector-General of Intelligence and Security Act 1986*.

Note: A defendant bears an evidential burden in relation to the matter in subsection (6) (see subsection 13.3(3) of the *Criminal Code*).

181B Disclosure/use offences: certain authorisations under Division 4

Disclosures

- (1) A person commits an offence if:
- (a) the person discloses information; and
 - (b) the information is about any of the following:
 - (i) whether an authorisation under Division 4 (other than under section 178A) has been, or is being, sought;
 - (ii) the making of such an authorisation;
 - (iii) the existence or non-existence of such an authorisation;
 - (iv) the revocation of such an authorisation;
 - (v) the notification of such a revocation.

Penalty: Imprisonment for 2 years.

- (2) A person commits an offence if:
- (a) the person discloses a document; and
 - (b) the document consists (wholly or partly) of any of the following:
 - (i) an authorisation under Division 4 (other than under section 178A);
 - (ii) the revocation of such an authorisation;
 - (iii) the notification of such a revocation.

Penalty: Imprisonment for 2 years.

- (3) Paragraphs (1)(a) and (2)(a) do not apply to a disclosure of information or a document if:
- (a) the disclosure is for the purposes of the authorisation, revocation or notification concerned; or
 - (b) the disclosure is reasonably necessary:
 - (i) to enable the Organisation to perform its functions; or
 - (ia) to enable a person to comply with his or her obligations under section 185D or 185E; or
 - (ii) to enforce the criminal law; or
 - (iia) for the purposes of Division 105A of the *Criminal Code* (post-sentence orders); or
 - (iii) to enforce a law imposing a pecuniary penalty; or
 - (iv) to protect the public revenue.

Note: A defendant bears an evidential burden in relation to the matter in subsection (3) (see subsection 13.3(3) of the *Criminal Code*).

Uses

- (4) A person commits an offence if:
- (a) the person uses information; and
 - (b) the information is about any of the following:
 - (i) whether an authorisation under Division 4 (other than under section 178A) has been, or is being, sought;
 - (ii) the making of such an authorisation;
 - (iii) the existence or non-existence of such an authorisation;

Section 182

- (iv) the revocation of such an authorisation;
- (v) the notification of such a revocation.

Penalty: Imprisonment for 2 years.

- (5) A person commits an offence if:
- (a) the person uses a document; and
 - (b) the document consists (wholly or partly) of any of the following:
 - (i) an authorisation under Division 4 (other than under section 178A);
 - (ii) the revocation of such an authorisation;
 - (iii) the notification of such a revocation.

Penalty: Imprisonment for 2 years.

- (6) Paragraphs (4)(a) and (5)(a) do not apply to a use of information or a document if:
- (a) the use is for the purposes of the authorisation, revocation or notification concerned; or
 - (b) the use is reasonably necessary:
 - (ia) to enable a person to comply with his or her obligations under section 185D or 185E; or
 - (i) to enforce the criminal law; or
 - (iaa) for the purposes of Division 105A of the *Criminal Code* (post-sentence orders); or
 - (ii) to enforce a law imposing a pecuniary penalty; or
 - (iii) to protect the public revenue.

Note: A defendant bears an evidential burden in relation to the matter in subsection (6) (see subsection 13.3(3) of the *Criminal Code*).

182 Secondary disclosure/use offence: disclosures under Division 4

- (1) A person commits an offence if:
- (a) information or a document is disclosed to the person as permitted by Division 4 or 4A; and
 - (b) the person discloses or uses the information or document.

Penalty: Imprisonment for 2 years.

Exempt disclosures

- (2) Paragraph (1)(b) does not apply to a disclosure of non-missing person information if:
- (a) the disclosure is reasonably necessary:
 - (i) for a person to comply with his or her obligations under section 185D or 185E; or
 - (ii) for the performance by the Organisation of its functions; or
 - (iii) for the enforcement of the criminal law; or
 - (iiia) for the purposes of Division 105A of the *Criminal Code* (post-sentence orders); or
 - (iv) for the enforcement of a law imposing a pecuniary penalty; or
 - (v) for the protection of the public revenue; or
 - (b) the disclosure is:
 - (i) to an IGIS official for the purpose of the Inspector-General of Intelligence and Security exercising powers, or performing functions or duties, under the *Inspector-General of Intelligence and Security Act 1986*; or
 - (ii) by an IGIS official in connection with the IGIS official exercising powers, or performing functions or duties, under that Act.

Note: A defendant bears an evidential burden in relation to the matter in subsection (2) (see subsection 13.3(3) of the *Criminal Code*).

- (2A) Paragraph (1)(b) does not apply to a disclosure of missing person information in relation to a missing person if:
- (a) the disclosure is reasonably necessary for the purposes of finding the missing person; or
 - (b) the information is disclosed to the person who notified the Australian Federal Police, or a Police Force of a State, of the missing person and:

Section 182

- (i) the missing person consented to the disclosure; or
- (ii) the missing person is unable to consent, and the disclosure is reasonably necessary to prevent a threat to the missing person's health, life or safety; or
- (iii) the missing person is dead.

Note: A defendant bears an evidential burden in relation to the matter in subsection (2A) (see subsection 13.3(3) of the *Criminal Code*).

Exempt uses

- (3) Paragraph (1)(b) does not apply to a use of non-missing person information if:
- (a) the use is reasonably necessary:
 - (i) for a person to comply with his or her obligations under section 185D or 185E; or
 - (ii) for the enforcement of the criminal law; or
 - (ia) for the purposes of Division 105A of the *Criminal Code* (post-sentence orders); or
 - (iii) for the enforcement of a law imposing a pecuniary penalty; or
 - (iv) for the protection of the public revenue; or
 - (b) the use is by an IGIS official in connection with the IGIS official exercising powers, or performing functions or duties, under the *Inspector-General of Intelligence and Security Act 1986*.

Note: A defendant bears an evidential burden in relation to the matter in subsection (3) (see subsection 13.3(3) of the *Criminal Code*).

- (4) Paragraph (1)(b) does not apply to a use of missing person information in relation to a missing person if the use is reasonably necessary for the purposes of finding the missing person.

Note: A defendant bears an evidential burden in relation to the matter in subsection (4) (see subsection 13.3(3) of the *Criminal Code*).

- (4A) Paragraph (1)(b) does not apply to a disclosure or use of information or a document if the disclosure or use is permitted by section 180C or 180D.

Note: A defendant bears an evidential burden in relation to the matter in subsection (4A) (see subsection 13.3(3) of the *Criminal Code*).

(5) In this Act:

missing person information, in relation to a missing person, means information or a document that is disclosed under section 178A (locating missing persons) in relation to the person who the Australian Federal Police, or a Police Force of a State, has been notified is missing.

non-missing person information means information or a document that is disclosed as permitted by Division 4 or 4A, but not under section 178A (locating missing persons).

182A Disclosure/use offences: journalist information warrants

- (1) A person commits an offence if:
- (a) the person discloses or uses information; and
 - (b) the information is about any of the following:
 - (i) whether a journalist information warrant (other than such a warrant that relates only to section 178A) has been, or is being, requested or applied for;
 - (ii) the making of such a warrant;
 - (iii) the existence or non-existence of such a warrant;
 - (iv) the revocation of such a warrant.

Penalty: Imprisonment for 2 years.

- (2) A person commits an offence if:
- (a) the person discloses or uses a document; and
 - (b) the document consists (wholly or partly) of any of the following:
 - (i) a journalist information warrant (other than such a warrant that relates only to section 178A);
 - (ii) the revocation of such a warrant.

Penalty: Imprisonment for 2 years.

Section 182B

182B Permitted disclosure or use: journalist information warrants

Paragraphs 182A(1)(a) and (2)(a) do not apply to a disclosure or use of information or a document if:

- (a) the disclosure or use is for the purposes of the warrant, revocation or notification concerned; or
- (b) the disclosure or use is reasonably necessary:
 - (i) to enable the making of submissions under section 180X; or
 - (ii) to enable a person to comply with his or her obligations under section 185D or 185E; or
 - (iii) to enable the Organisation to perform its functions; or
 - (iv) to enforce the criminal law; or
- (iva) for the purposes of Division 105A of the *Criminal Code* (post-sentence orders); or
- (v) to enforce a law imposing a pecuniary penalty; or
- (vi) to protect the public revenue; or
- (c) in the case of a disclosure—the disclosure is:
 - (i) to an IGIS official for the purpose of the Inspector-General of Intelligence and Security exercising powers, or performing functions or duties, under the *Inspector-General of Intelligence and Security Act 1986*; or
 - (ii) by an IGIS official in connection with the IGIS official exercising powers, or performing functions or duties, under that Act; or
- (d) in the case of a use—the use is by an IGIS official in connection with the IGIS official exercising powers, or performing functions or duties, under the *Inspector-General of Intelligence and Security Act 1986*.

Note: A defendant bears an evidential burden in relation to the matter in this section (see subsection 13.3(3) of the *Criminal Code*).

Part 4-2—Procedural requirements relating to authorisations

183 Form of authorisations and notifications

- (1) The following:
 - (a) an authorisation under Division 3, 4 or 4A of Part 4-1;
 - (b) the notification of such an authorisation;
 - (c) the revocation of such an authorisation;
 - (d) the notification of such a revocation;must:
 - (e) be in written form or in electronic form (for example, email);
and
 - (f) comply with such requirements as are determined under subsection (2).
- (2) The Communications Access Co-ordinator may, by legislative instrument, determine requirements for the purposes of paragraph (1)(f).
- (3) The Co-ordinator must consult the ACMA and the Information Commissioner in relation to matters that relate to the privacy functions (within the meaning of the *Australian Information Commissioner Act 2010*) before making a determination under subsection (2).

184 Notification of authorisations or revocations

The Organisation

- (1) If a person makes an authorisation under Division 3 of Part 4-1, an ASIO employee or ASIO affiliate must notify the person from whom the disclosure is sought.

Section 185

- (2) If, under subsection 176(6), a person revokes an authorisation, an ASIO employee or ASIO affiliate must notify the person who was notified of the authorisation.

Enforcement agencies

- (3) If an authorised officer of an enforcement agency makes an authorisation under Division 4 of Part 4-1, a relevant staff member of the enforcement agency must notify the person from whom the disclosure is sought.
- (4) If, under subsection 180(7), an authorised officer of a criminal law-enforcement agency revokes an authorisation, a relevant staff member of the enforcement agency must notify the person who was notified of the authorisation.

Authorised officers of the Australian Federal Police

- (5) If an authorised officer of the Australian Federal Police makes an authorisation under subsection 180A(2) or 180B(2), or extends the period for which an authorisation is in force under subsection 180B(6), a relevant staff member of the Australian Federal Police must notify the person from whom the disclosure is sought.
- (6) If, under subsection 180B(4), an authorised officer of the Australian Federal Police revokes an authorisation, a relevant staff member of the Australian Federal Police must notify the person who was notified of the authorisation.

185 Retention of authorisations

- (1) The head (however described) of an enforcement agency must retain an authorisation made under Division 4 of Part 4-1 by an authorised officer of the enforcement agency for the period of 3 years beginning on the day the authorisation is made.
- (2) The Commissioner of Police must retain an authorisation made under Division 4A of Part 4-1 by an authorised officer of the

Australian Federal Police for the period of 3 years beginning on the day the authorisation is made.

- (3) This section does not limit subsection 187N(3).

185A Evidentiary certificates relating to acts by carriers

- (1) The following:
- (a) the Managing Director of a carrier or a body corporate of which the carrier is a subsidiary;
 - (b) the secretary of a carrier or a body corporate of which the carrier is a subsidiary;
 - (c) an employee of a carrier authorised in writing for the purposes of this paragraph by a person referred to in paragraph (a) or (b);
- may issue a written certificate signed by him or her setting out such facts as he or she considers relevant with respect to acts or things done by, or in relation to, employees of the carrier in order to enable the disclosure of information or a document covered by an authorisation in force under a provision of Division 3 or 4 of Part 4-1.
- (2) A document purporting to be a certificate issued under subsection (1) and purporting to be signed by a person referred to in paragraph (a), (b) or (c) of that subsection:
- (a) is to be received in evidence in an exempt proceeding without further proof; and
 - (b) is, in an exempt proceeding, conclusive evidence of the matters stated in the document.
- (3) For the purposes of this section, the question whether a body corporate is a subsidiary of another body corporate is to be determined in the same manner as the question is determined under the *Corporations Act 2001*.

Section 185B

185B Evidentiary certificates relating to acts by the Organisation

- (1) The Director-General of Security or the Deputy Director-General of Security may issue a written certificate signed by him or her setting out such facts as he or she considers relevant with respect to:
 - (a) anything done by an ASIO employee or ASIO affiliate in connection with the disclosure of information or a document covered by an authorisation in force under a provision of Division 3 or 4 of Part 4-1; or
 - (b) anything done by an ASIO employee or ASIO affiliate in connection with:
 - (i) the communication by a person to another person of information, or information contained in a document, covered by such an authorisation; or
 - (ii) the making use of such information; or
 - (iii) the making of a record of such information; or
 - (iv) the custody of a record of such information; or
 - (v) the giving in evidence of such information.
- (2) A document purporting to be a certificate issued under subsection (1) by the Director-General of Security or the Deputy Director-General of Security and to be signed by him or her:
 - (a) is to be received in evidence in an exempt proceeding without further proof; and
 - (b) is, in an exempt proceeding, prima facie evidence of the matters stated in the document.

185C Evidentiary certificates relating to acts by enforcement agencies

- (1) A certifying officer of an enforcement agency may issue a written certificate signed by him or her setting out such facts as he or she considers relevant with respect to:
 - (a) anything done by an officer or staff member of the agency in connection with the disclosure of information or a document

- covered by an authorisation in force under a provision of Division 3 or 4 of Part 4-1; or
- (b) anything done by an officer or staff member of the agency in connection with:
- (i) the communication by a person to another person of information, or information contained in a document, covered by such an authorisation; or
 - (ii) the making use of such information; or
 - (iii) the making of a record of such information; or
 - (iv) the custody of a record of such information; or
 - (v) the giving in evidence of such information.
- (2) A document purporting to be a certificate issued under subsection (1) by a certifying officer of an enforcement agency and to be signed by him or her:
- (a) is to be received in evidence in an exempt proceeding without further proof; and
 - (b) is, in an exempt proceeding, prima facie evidence of the matters stated in the document.

185D Notification etc. of authorisations intended to identify media sources

The Organisation

- (1) If a journalist information warrant is issued under Subdivision B of Division 4C of Part 4-1:
- (a) the Director-General of Security must, as soon as practicable, give a copy of the warrant to the Inspector-General of Intelligence and Security; and
 - (b) the Attorney-General must, as soon as practicable, cause the Parliamentary Joint Committee on Intelligence and Security to be notified of the issuing of the warrant.
- (2) If an authorisation under Division 3 of Part 4-1 is made under the authority of the warrant, the Director-General of Security must, as soon as practicable after the expiry of the warrant, give a copy of

Section 185D

the authorisation to the Inspector-General of Intelligence and Security.

- (3) If:
- (a) the Inspector-General gives to the Minister a report under section 22 or 25A of the *Inspector-General of Intelligence and Security Act 1986*; and
 - (b) the report relates (wholly or partly) to one or both of the following:
 - (i) a journalist information warrant issued to the Organisation;
 - (ii) one or more authorisations referred to in subsection (2) of this section;
- the Minister must, as soon as practicable, cause a copy of the report to be given to the Parliamentary Joint Committee on Intelligence and Security.
- (4) The Parliamentary Joint Committee on Intelligence and Security may request a briefing from the Inspector-General on:
- (a) a journalist information warrant; or
 - (b) an authorisation or authorisations;
- to which a report referred to in paragraph (3)(b) of this section relates.

Enforcement agencies

- (5) If a journalist information warrant is issued to an enforcement agency:
- (a) if the agency was the Australian Federal Police:
 - (i) the Commissioner of Police must, as soon as practicable, give copies of the warrant to the Minister and the Ombudsman; and
 - (ii) the Minister must, as soon as practicable after receiving a copy, cause the Parliamentary Joint Committee on Intelligence and Security to be notified of the issuing of the warrant; and

Section 185E

- (b) otherwise—the chief officer of the agency must, as soon as practicable, give a copy of the warrant to the Ombudsman.
- (6) If an authorisation under Division 4 of Part 4-1 is made under the authority of the warrant, the chief officer of the agency must, as soon as practicable after the expiry of the warrant, give a copy of the authorisation to the Ombudsman.
- (7) If:
 - (a) the Ombudsman gives to the Minister a report under section 186J of this Act; and
 - (b) the report relates (wholly or partly) to one or both of the following:
 - (i) a journalist information warrant issued to the Australian Federal Police;
 - (ii) one or more authorisations, referred to in subsection (6) of this section, that were made by one or more authorised officers of the Australian Federal Police;the Minister must, as soon as practicable, cause a copy of the report to be given to the Parliamentary Joint Committee on Intelligence and Security.
- (8) The Parliamentary Joint Committee on Intelligence and Security may request a briefing from the Ombudsman on:
 - (a) a journalist information warrant; or
 - (b) an authorisation or authorisations;to which a report referred to in paragraph (7)(b) of this section relates.

185E Reports on access to retained data

The Organisation

- (1) If:
 - (a) the Inspector-General of Intelligence and Security gives to the Minister a report under section 22 or 25A of the *Inspector-General of Intelligence and Security Act 1986*; and

Section 186

- (b) the report relates (wholly or partly) to the purpose or manner of access to retained data by means of one or more authorisations under Division 3 of Part 4-1 of this Act; the Minister must, as soon as practicable, cause a copy of the report to be given to the Parliamentary Joint Committee on Intelligence and Security.
- (2) The Parliamentary Joint Committee on Intelligence and Security may request a briefing from the Inspector-General on the authorisation or authorisations.

Australian Federal Police

- (3) If:
 - (a) the Ombudsman gives to the Minister a report under section 186J of this Act; and
 - (b) the report relates (wholly or partly) to the purpose or manner of access to retained data by means of one or more authorisations under Division 4 or 4A of Part 4-1 of this Act; and
 - (c) the authorisation or authorisations were made by one or more authorised officers of the Australian Federal Police;the Minister must, as soon as practicable, cause a copy of the report to be given to the Parliamentary Joint Committee on Intelligence and Security.
- (4) The Parliamentary Joint Committee on Intelligence and Security may request a briefing from the Ombudsman on the authorisation or authorisations.

186 Report to Minister

- (1) As soon as practicable, and in any event within 3 months, after each 30 June, the head (however described) of an enforcement agency must give the Minister a written report that relates to the year ending on that 30 June and that sets out:

Section 186

- (a) the number of authorisations made under section 178 by an authorised officer of the enforcement agency during that year; and
- (aa) the number of authorisations made under section 178A by an authorised officer of the enforcement agency during that year; and
- (b) the number of authorisations made under section 179 by an authorised officer of the enforcement agency during that year; and
- (c) for a criminal law-enforcement agency—the number of authorisations made under section 180 by an authorised officer of the enforcement agency during that year; and
- (ca) if the enforcement agency is the Australian Federal Police—the number of authorisations made under sections 180A, 180B, 180C and 180D by an authorised officer of the Australian Federal Police during that year; and
- (cb) if the enforcement agency is the Australian Federal Police, and information or documents were disclosed, under an authorisation referred to in paragraph (ca), by an authorised officer of the Australian Federal Police during that year to one or more foreign countries:
 - (i) the name of each such country; and
 - (ii) the number of disclosures under such authorisations; and
- (d) any other matter requested by the Minister in relation to those authorisations; and
- (e) the offences and other matters for which authorised officers of the agency made authorisations under sections 178, 178A, 179 and 180 during that year; and
- (f) the lengths of time for which the information or documents that were covered by those authorisations had been held when the authorisations were made; and
- (g) the number of occasions during that year on which authorised officers of the agency made authorisations relating to retained data that included information of a kind referred to in item 1 of the table in subsection 187AA(1); and

Section 186

- (h) the number of occasions during that year on which authorised officers of the agency made authorisations relating to retained data that included information of a kind referred to in item 2, 3, 4, 5 or 6 of the table in subsection 187AA(1); and
 - (i) the number of authorisations, referred to in paragraph (e) of this subsection, that were made under journalist information warrants issued to the agency under Subdivision C of Division 4C of Part 4-1; and
 - (j) the number of journalist information warrants issued to the agency under that Subdivision during the period; and
 - (k) information of a kind declared under subsection (1E) of this section.
- (1A) The report under subsection (1) is to set out the offences and other matters referred to in paragraph (1)(e) by means of the categories declared under subsection (1B).
- (1B) The Minister may, by legislative instrument, declare categories of offences and other matters into which the offences and other matters are to be divided for the purposes of paragraph (1)(e).
- (1C) The report under subsection (1) is to set out the matters referred to in paragraph (1)(f) by specifying:
- (a) in relation to each of 8 successive periods of 3 months, the number of the authorisations made for information or documents held for lengths of time included in that period; and
 - (b) the number of the authorisations made for information or documents held for lengths of time exceeding 24 months.
- (1D) For the purposes of paragraph (1)(f), disregard any authorisations under subsection 180(2), except to the extent that they include authorisations under subsection 180(3).
- (1E) The Minister may, by legislative instrument, declare kinds of information that are to be set out in the report under subsection (1).

- (2) The Minister must prepare a report that contains the information set out in each report under subsection (1), other than the information referred to in paragraph (1)(cb). The report may contain any other information the Minister considers appropriate.
- (3) The Minister must cause a copy of a report under subsection (2) to be laid before each House of the Parliament within 15 sitting days of that House after the day on which the report was completed.
- (4) A report under this section must not be made in a manner that is likely to enable the identification of a person.

186A Obligation to keep records

- (1) The chief officer of an enforcement agency must cause the following, or copies of the following, to be kept in the agency's records for the period specified in subsection (3):
 - (a) each authorisation made by an authorised officer of the agency under section 178, 178A, 179 or 180, and documents or other materials that indicate any of the following:
 - (i) whether the authorisation was properly made (including whether the authorised officer took into account the matters referred to in subsection 178(3), 178A(3), 179(3) or 180(4) (as the case requires), the matters referred to in section 180F and all other relevant considerations);
 - (ii) if the authorisation is made under section 180—the period during which the authorisation is in force;
 - (iii) when the authorisation was notified under subsection 184(3);
 - (b) each notice of the revocation under subsection 180(7) of an authorisation under section 180, and documents or other materials that indicate any of the following:
 - (i) whether the revocation was properly made;
 - (ii) when the revocation was notified under subsection 184(4);

Section 186A

- (c) if the agency is the Australian Federal Police—each authorisation made by an authorised officer of the Australian Federal Police under section 180A or 180B, and documents or other materials that indicate any of the following:
 - (i) whether the authorisation was properly made (including whether the authorised officer took into account the matters referred to in subsection 180A(3) or (5), 180B(3) or (8) or 180E(1) (as the case requires), the matters referred to in section 180F and all other relevant considerations);
 - (ii) if the authorisation is made under section 180B—the period during which the authorisation is in force;
 - (iii) if the authorisation is made under subsection 180B(8)—whether the authorised officer was satisfied as to the matters referred to in paragraphs 180B(8)(a) and (b);
 - (iv) when the authorisation was notified under subsection 184(5);
- (d) if the agency is the Australian Federal Police—each notice of the extension under subsection 180B(6) of an authorisation under section 180B, and documents or other materials that indicate any of the following:
 - (i) whether the extension was properly made;
 - (ii) when the extension was notified under subsection 184(5);
- (e) if the agency is the Australian Federal Police—each notice of the revocation under subsection 180B(4) of an authorisation under section 180B, and documents or other materials that indicate any of the following:
 - (i) whether the revocation was properly made;
 - (ii) when the revocation was notified under subsection 184(6);
- (f) if the agency is the Australian Federal Police—each authorisation made by an authorised officer of the Australian Federal Police under section 180C or 180D, and documents or other materials that indicate whether the authorisation was

properly made, including whether the authorised officer took into account:

- (i) the matters referred to in subsection 180C(2), 180D(2) or 180E(1) (as the case requires); and
 - (ii) the matters referred to in section 180F; and
 - (iii) all other relevant considerations;
- (g) documents or other materials that indicate whether:
- (i) a disclosure of information or a document to which subsection 181B(1) or (2) applies took place in circumstances referred to in subsection 181B(3); or
 - (ii) a use of information or a document to which subsection 181B(4) or (5) applies took place in circumstances referred to in subsection 181B(6); or
 - (iii) a disclosure or use of information or a document to which subsection 182(1) applies took place in circumstances referred to in subsection 182(2), (2A), (3), (4) or (4A);
- (h) each evidentiary certificate issued under section 185C;
- (i) each report given to the Minister under section 186;
- (j) documents and other materials of a kind prescribed under subsection (2) of this section.
- (2) The Minister may, by legislative instrument, prescribe kinds of documents and other materials that the chief officer of an enforcement agency must cause to be kept in the agency's records.
- (3) The period for which the chief officer of an enforcement agency must cause a particular item to be kept in the agency's records under subsection (1) of this section is the period:
- (a) starting when the item came into existence; and
 - (b) ending:
 - (i) when 3 years have elapsed since the item came into existence; or
 - (ii) when the Ombudsman gives a report to the Minister under section 186J that is about records that include the item;

Section 186A

whichever happens earlier.

(4) Subsection (3) does not affect the operation of section 185.

Chapter 4A—Oversight by the Commonwealth Ombudsman

186B Inspection of records

- (1) The Ombudsman must inspect records of an enforcement agency to determine:
 - (a) the extent of compliance with Chapter 4 by the agency and its officers; and
 - (b) if the agency is a criminal law-enforcement agency—the extent of compliance with Chapter 3 by the agency and its officers.
- (1A) If:
 - (a) the performance of a function, or the exercise of a power, conferred by Part 15 of the *Telecommunications Act 1997* is in connection with:
 - (i) a stored communications warrant; or
 - (ii) an authorisation under Division 3, 4 or 4A of Part 4-1; and
 - (b) an enforcement agency has records that relate to the performance of that function or the exercise of that power; the Ombudsman may inspect those records in order to determine the extent of compliance with Part 15 of the *Telecommunications Act 1997* by the agency and its officers.
- (2) For the purpose of an inspection under this section, the Ombudsman:
 - (a) after notifying the chief officer of the agency, may enter at any reasonable time premises occupied by the agency; and
 - (b) is entitled to have full and free access at all reasonable times to all records of the agency that are relevant to the inspection; and
 - (c) despite any other law, is entitled to make copies of, and to take extracts from, records of the agency; and

Section 186C

- (d) may require a member of staff of the agency to give the Ombudsman any information that the Ombudsman considers necessary, being information:
 - (i) that is in the member's possession, or to which the member has access; and
 - (ii) that is relevant to the inspection.
- (3) Before inspecting records of an enforcement agency under this section, the Ombudsman must give reasonable notice to the chief officer of the agency of when the inspection will occur.
- (4) The chief officer must ensure that members of staff of the agency give the Ombudsman any assistance the Ombudsman reasonably requires to enable the Ombudsman to perform functions under this section.
- (5) To avoid doubt, subsection (1) does not require the Ombudsman to inspect all of the records of an enforcement agency that are relevant to the matters referred to in paragraphs (1)(a) and (b).
- (6) While an operation is being conducted under:
 - (a) a stored communications warrant; or
 - (b) an authorisation under Division 3, 4 or 4A of Part 4-1;the Ombudsman may refrain from inspecting any records of the agency concerned that are relevant to the obtaining or execution of the warrant or authorisation.

186C Power to obtain relevant information

- (1) If the Ombudsman has reasonable grounds to believe that an officer of a particular enforcement agency is able to give information relevant to an inspection under this Chapter of the agency's records, the Ombudsman may:
 - (a) if the Ombudsman knows the officer's identity—by writing given to the officer, require the officer to do one or both of the following:

- (i) give the information to the Ombudsman, by writing signed by the officer, at a specified place and within a specified period;
 - (ii) attend before a specified inspecting officer to answer questions relevant to the inspection; or
 - (b) if the Ombudsman does not know the officer's identity—require the chief officer of the agency, or a person nominated by the chief officer, to attend before a specified inspecting officer to answer questions relevant to the inspection.
- (2) A requirement under subsection (1) to attend before an inspecting officer must specify:
- (a) a place for the attendance; and
 - (b) a period within which, or a time and day when, the attendance is to occur.
- The place, and the period or the time and day, must be reasonable having regard to the circumstances in which the requirement is made.
- (3) A person must not refuse:
- (a) to attend before a person; or
 - (b) to give information; or
 - (c) to answer questions;
- when required to do so under this section.

Penalty for an offence against this subsection: Imprisonment for 6 months.

186D Ombudsman to be given information and access despite other laws

- (1) Despite any other law, a person is not excused from giving information, answering a question, or giving access to a document, as and when required under this Chapter, on the ground that giving the information, answering the question, or giving access to the document, as the case may be, would:
- (a) contravene a law; or

Section 186E

- (b) be contrary to the public interest; or
 - (c) might tend to incriminate the person or make the person liable to a penalty.
- (2) However:
 - (a) the information, the answer, or the fact that the person has given access to the document, as the case may be; and
 - (b) any information or thing (including a document) obtained as a direct or indirect consequence of giving the information, answering the question or giving access to the document;is not admissible in evidence against the person except in a proceeding by way of a prosecution for an offence against section 133, 181A, 181B or 182, or against Part 7.4 or 7.7 of the *Criminal Code*.
- (3) Nothing in section 133, 181A, 181B or 182, or in any other law, prevents an officer of an enforcement agency from:
 - (a) giving information to an inspecting officer (whether orally or in writing and whether or not in answer to a question); or
 - (b) giving access to a record of the agency to an inspecting officer;for the purposes of an inspection under this Chapter of the agency's records.
- (4) Nothing in section 133, 181A, 181B or 182, or in any other law, prevents an officer of an enforcement agency from making a record of information, or causing a record of information to be made, for the purposes of giving the information to a person as permitted by subsection (3).

186E Application of Ombudsman Act

- (1) Section 11A of the *Ombudsman Act 1976* does not apply in relation to the exercise or proposed exercise of a power, or the performance or the proposed performance of a function, of the Ombudsman under this Chapter.

- (2) A reference in section 19 of the *Ombudsman Act 1976* to the Ombudsman's operations does not include a reference to anything that an inspecting officer has done or omitted to do under this Chapter.
- (3) Subject to section 186D of this Act, subsections 35(2), (3), (4) and (8) of the *Ombudsman Act 1976* apply for the purposes of this Chapter and so apply as if:
 - (a) a reference in those subsections to an officer were a reference to an inspecting officer; and
 - (b) a reference in those subsections to information did not include a reference to lawfully accessed information or lawfully intercepted information; and
 - (c) a reference in those subsections to that Act were a reference to this Chapter; and
 - (d) paragraph 35(3)(b) of that Act were omitted; and
 - (e) section 35A of that Act had not been enacted.

186F Exchange of information between Ombudsman and State inspecting authorities

- (1) If the Ombudsman has obtained under this Act information relating to an authority of a State or Territory, the Ombudsman may give the information to another authority of that State or Territory (an *inspecting authority*) that:
 - (a) has powers under the law of that State or Territory; and
 - (b) has the function of making inspections of a similar kind to those provided for in section 186B of this Act when the inspecting authority is exercising those powers.
- (2) However, the Ombudsman may give the information only if the Ombudsman is satisfied that giving the information is necessary to enable the inspecting authority to perform its functions in relation to the authority of the State or Territory.
- (3) The Ombudsman may receive, from an inspecting authority, information relevant to the performance of the Ombudsman's functions under this Act.

Section 186G

186G Delegation by Ombudsman

- (1) The Ombudsman may delegate:
 - (a) to an APS employee responsible to the Ombudsman; or
 - (b) to a person having similar oversight functions to the Ombudsman under the law of a State or Territory or to an employee responsible to that person;all or any of the Ombudsman's powers under this Chapter other than a power to report to the Minister.
- (2) A delegate must, upon request by a person affected by the exercise of any power delegated to the delegate, produce the instrument of delegation, or a copy of the instrument, for inspection by the person.

186H Ombudsman not to be sued

The Ombudsman, an inspecting officer, or a person acting under an inspecting officer's direction or authority, is not liable to an action, suit or proceeding for or in relation to an act done, or omitted to be done, in good faith in the performance or exercise, or the purported performance or exercise, of a function or power conferred by this Chapter.

186J Reports

- (1) The Ombudsman must report to the Minister, in writing, about the results of inspections under section 186B of the records of agencies during a financial year.
- (2) The report under subsection (1) must be given to the Minister as soon as practicable after the end of the financial year.
- (3) The Minister must cause a copy of the report to be laid before each House of the Parliament within 15 sitting days of that House after the Minister receives it.

- (4) The Ombudsman may report to the Minister in writing at any time about the results of an inspection under this Chapter and must do so if so requested by the Minister.
- (5) If, as a result of an inspection under this Chapter of the records of an enforcement agency, the Ombudsman is of the opinion that an officer of the agency has contravened a provision of this Act, the Ombudsman may include in his or her report on the inspection a report on the contravention.

Note: In complying with this section, the Ombudsman remains bound by the obligations imposed by sections 133, 181B and 182.

- (6) The Ombudsman must give a copy of a report under subsection (1) or (4) to the chief officer of any enforcement agency to which the report relates.
- (7) A report under this section must not include information which, if made public, could reasonably be expected to:
 - (a) endanger a person's safety; or
 - (b) prejudice an investigation or prosecution; or
 - (c) compromise any enforcement agency's operational activities or methodologies.

Chapter 5—Co-operation with agencies

Part 5-1—Definitions

187 Definitions

- (1) This section sets out the meaning of the following 2 important concepts used in this Chapter:
 - (a) interception capability (relating to obligations under Part 5-3);
 - (b) delivery capability (relating to obligations under Part 5-5).These concepts do not overlap.

Interception capability

- (2) In this Chapter, ***interception capability***, in relation to a particular kind of telecommunications service that involves, or will involve, the use of a telecommunications system, means the capability of that kind of service or of that system to enable:
 - (a) a communication passing over the system to be intercepted; and
 - (b) lawfully intercepted information to be transmitted to the delivery points applicable in respect of that kind of service.

Delivery capability

- (3) In this Chapter, ***delivery capability***, in relation to a particular kind of telecommunications service that involves, or will involve, the use of a telecommunications system, means the capability of that kind of service or of that system to enable lawfully intercepted information to be delivered to interception agencies from the delivery points applicable in respect of that kind of service.

Part 5-1A—Data retention

Division 1—Obligation to keep information and documents

187A Service providers must keep certain information and documents

- (1) A person (a *service provider*) who operates a service to which this Part applies (a *relevant service*) must keep, or cause to be kept, in accordance with section 187BA and for the period specified in section 187C:

- (a) information of a kind specified in or under section 187AA; or
- (b) documents containing information of that kind;

relating to any communication carried by means of the service.

Note 1: Subsection (3) sets out the services to which this Part applies.

Note 2: Section 187B removes some service providers from the scope of this obligation, either completely or in relation to some services they operate.

Note 3: Division 3 provides for exemptions from a service provider's obligations under this Part.

- (3) This Part applies to a service if:
- (a) it is a service for carrying communications, or enabling communications to be carried, by means of guided or unguided electromagnetic energy or both; and
 - (b) it is a service:
 - (i) operated by a carrier; or
 - (ii) operated by an internet service provider (within the meaning of the *Online Safety Act 2021*); or
 - (iii) of a kind for which a declaration under subsection (3A) is in force; and
 - (c) the person operating the service owns or operates, in Australia, infrastructure that enables the provision of any of its relevant services;

Section 187A

but does not apply to a broadcasting service (within the meaning of the *Broadcasting Services Act 1992*).

- (3A) The Minister may, by legislative instrument, declare a service to be a service to which this Part applies.
- (3B) A declaration under subsection (3A):
- (a) comes into force when it is made, or on such later day as is specified in the declaration; and
 - (b) ceases to be in force at the end of the period of 40 sitting days of a House of the Parliament after the declaration comes into force.
- (3C) If a Bill is introduced into either House of the Parliament that includes an amendment of subsection (3), the Minister:
- (a) must refer the amendment to the Parliamentary Joint Committee on Intelligence and Security for review; and
 - (b) must not in that referral specify, as the period within which the Committee is to report on its review, a period that will end earlier than 15 sitting days of a House of the Parliament after the introduction of the Bill.
- (4) This section does not require a service provider to keep, or cause to be kept:
- (a) information that is the contents or substance of a communication; or
- Note: This paragraph puts beyond doubt that service providers are not required to keep information about telecommunications content.
- (b) information that:
 - (i) states an address to which a communication was sent on the internet, from a telecommunications device, using an internet access service provided by the service provider; and
 - (ii) was obtained by the service provider only as a result of providing the service; or
- Note: This paragraph puts beyond doubt that service providers are not required to keep information about subscribers' web browsing history.

- (c) information to the extent that it relates to a communication that is being carried by means of another service:
 - (i) that is of a kind referred to in paragraph (3)(a); and
 - (ii) that is operated by another person using the relevant service operated by the service provider;or a document to the extent that the document contains such information; or

Note: This paragraph puts beyond doubt that service providers are not required to keep information or documents about communications that pass “over the top” of the underlying service they provide, and that are being carried by means of other services operated by other service providers.

- (d) information that the service provider is required to delete because of a determination made under section 99 of the *Telecommunications Act 1997*, or a document to the extent that the document contains such information; or
 - (e) information about the location of a telecommunications device that is not information used by the service provider in relation to the relevant service to which the device is connected.
- (5) Without limiting subsection (1), for the purposes of this section:
- (a) an attempt to send a communication by means of a relevant service is taken to be the sending of a communication by means of the service, if the attempt results in:
 - (i) a connection between the telecommunications device used in the attempt and another telecommunications device; or
 - (ii) an attempted connection between the telecommunications device used in the attempt and another telecommunications device; or
 - (iii) a conclusion being drawn, through the operation of the service, that a connection cannot be made between the telecommunications device used in the attempt and another telecommunications device; and
 - (b) an untariffed communication by means of a relevant service is taken to be a communication by means of the service.

Chapter 5 Co-operation with agencies

Part 5-1A Data retention

Division 1 Obligation to keep information and documents

Section 187AA

- (6) To avoid doubt, if information that subsection (1) requires a service provider to keep in relation to a communication is not created by the operation of a relevant service, subsection (1) requires the service provider to use other means to create the information, or a document containing the information.

187AA Information to be kept

- (1) The following table sets out the kinds of information that a service provider must keep, or cause to be kept, under subsection 187A(1):

Kinds of information to be kept		
Item	Topic Column 1	Description of information Column 2
1	The subscriber of, and accounts, services, telecommunications devices and other relevant services relating to, the relevant service	<p>The following:</p> <p>(a) any information that is one or both of the following:</p> <ul style="list-style-type: none">(i) any name or address information;(ii) any other information for identification purposes; <p>relating to the relevant service, being information used by the service provider for the purposes of identifying the subscriber of the relevant service;</p> <p>(b) any information relating to any contract, agreement or arrangement relating to the relevant service, or to any related account, service or device;</p> <p>(c) any information that is one or both of the following:</p> <ul style="list-style-type: none">(i) billing or payment information;(ii) contact information; <p>relating to the relevant service, being information used by the service provider in relation to the relevant service;</p> <p>(d) any identifiers relating to the relevant service or any related account, service or device, being information used by the service provider in</p>

Section 187AA

Kinds of information to be kept		
Item	Topic Column 1	Description of information Column 2
		relation to the relevant service or any related account, service or device; (e) the status of the relevant service, or any related account, service or device.
2	The source of a communication	Identifiers of a related account, service or device from which the communication has been sent by means of the relevant service.
3	The destination of a communication	Identifiers of the account, telecommunications device or relevant service to which the communication: (a) has been sent; or (b) has been forwarded, routed or transferred, or attempted to be forwarded, routed or transferred.
4	The date, time and duration of a communication, or of its connection to a relevant service	The date and time (including the time zone) of the following relating to the communication (with sufficient accuracy to identify the communication): (a) the start of the communication; (b) the end of the communication; (c) the connection to the relevant service; (d) the disconnection from the relevant service.
5	The type of a communication or of a relevant service used in connection with a communication	The following: (a) the type of communication; Examples: Voice, SMS, email, chat, forum, social media. (b) the type of the relevant service; Examples: ADSL, Wi-Fi, VoIP, cable, GPRS, VoLTE, LTE. (c) the features of the relevant service that were, or would have been, used by or enabled for the communication. Examples: Call waiting, call forwarding, data volume usage.

Chapter 5 Co-operation with agencies

Part 5-1A Data retention

Division 1 Obligation to keep information and documents

Section 187AA

Kinds of information to be kept

Item	Topic Column 1	Description of information Column 2
		Note: This item will only apply to the service provider operating the relevant service: see paragraph 187A(4)(c).
6	The location of equipment, or a line, used in connection with a communication	The following in relation to the equipment or line used to send or receive the communication: (a) the location of the equipment or line at the start of the communication; (b) the location of the equipment or line at the end of the communication. Examples: Cell towers, Wi-Fi hotspots.

- (2) The Minister may, by legislative instrument, make a declaration modifying (including by adding, omitting or substituting) the table in subsection (1), or that table as previously modified under this subsection.
- (3) A declaration under subsection (2):
- (a) comes into force when it is made, or on such later day as is specified in the declaration; and
 - (b) ceases to be in force at the end of the period of 40 sitting days of a House of the Parliament after the declaration comes into force.
- (4) If a Bill is introduced into either House of the Parliament that includes an amendment of subsection 187A(4) or subsection (1) or (5) of this section, the Minister:
- (a) must refer the amendment to the Parliamentary Joint Committee on Intelligence and Security for review; and
 - (b) must not in that referral specify, as the period within which the Committee is to report on its review, a period that will end earlier than 15 sitting days of a House of the Parliament after the introduction of the Bill.
-

- (5) For the purposes of items 2, 3, 4 and 6 of the table in subsection (1) and any modifications of those items under subsection (2), 2 or more communications that together constitute a single communications session are taken to be a single communication.

187B Certain service providers not covered by this Part

- (1) Subsection 187A(1) does not apply to a service provider (other than a carrier that is not a carriage service provider) in relation to a relevant service that it operates if:
- (a) the service:
 - (i) is provided only to a person's immediate circle (within the meaning of section 23 of the *Telecommunications Act 1997*); or
 - (ii) is provided only to places that, under section 36 of that Act, are all in the same area; and
 - (b) the service is not subject to a declaration under subsection (2) of this section.
- (2) The Communications Access Co-ordinator may declare that subsection 187A(1) applies in relation to a relevant service that a service provider operates.
- (2A) Before making the declaration, the Communications Access Co-ordinator may consult the Privacy Commissioner.
- (3) In considering whether to make the declaration, the Communications Access Co-ordinator must have regard to:
- (a) the interests of law enforcement and national security; and
 - (b) the objects of the *Telecommunications Act 1997*; and
 - (ba) the objects of the *Privacy Act 1988*; and
 - (bb) any submissions made by the Privacy Commissioner because of the consultation under subsection (2A); and
 - (c) any other matter that the Communications Access Co-ordinator considers relevant.
- (4) The declaration must be in writing.

Section 187BA

- (5) A declaration made under subsection (2) is not a legislative instrument.
- (6) As soon as practicable after making a declaration under subsection (2), the Communications Access Co-ordinator must give written notice of the declaration to the Minister.
- (7) As soon as practicable after receiving the notice under subsection (6), the Minister must give written notice of the declaration to the Parliamentary Joint Committee on Intelligence and Security.

187BA Ensuring the confidentiality of information

A service provider must protect the confidentiality of information that, or information in a document that, the service provider must keep, or cause to be kept, under section 187A by:

- (a) encrypting the information; and
- (b) protecting the information from unauthorised interference or unauthorised access.

187C Period for keeping information and documents

- (1) The period for which a service provider must keep, or cause to be kept, information or a document under section 187A is:
 - (a) if the information is about, or the document contains information about, a matter of a kind described in paragraph (a) or (b) in column 2 of item 1 of the table in subsection 187AA(1)—the period:
 - (i) starting when the information or document came into existence; and
 - (ii) ending 2 years after the closure of the account to which the information or document relates; or
 - (b) otherwise—the period:
 - (i) starting when the information or document came into existence; and
 - (ii) ending 2 years after it came into existence.

- (2) However, the regulations may prescribe that, in relation to a specified matter of a kind described in paragraph (a) or (b) in column 2 of item 1 of the table in subsection 187AA(1), the period under subsection (1) of this section is the period referred to in paragraph (1)(b) of this section.
- (3) This section does not prevent a service provider from keeping information or a document for a period that is longer than the period provided under this section.

Note: Division 3 provides for reductions in periods specified under this section.

Division 2—Data retention implementation plans

187D Effect of data retention implementation plans

While there is in force a data retention implementation plan for a relevant service operated by a service provider:

- (a) the service provider must comply with the plan in relation to communications carried by means of that service; but
- (b) the service provider is not required to comply with subsection 187A(1) (or section 187BA or 187C) in relation to those communications.

187E Applying for approval of data retention implementation plans

- (1) A service provider may apply to the Communications Access Co-ordinator for approval of a data retention implementation plan for one or more relevant services operated by the service provider.
- (2) The plan must specify, in relation to each such service:
 - (a) an explanation of the current practices for keeping, and ensuring the confidentiality of, information and documents that section 187A would require to be kept, if the plan were not in force; and
 - (b) details of the interim arrangements that the service provider proposes to be implemented, while the plan is in force, for keeping, and ensuring the confidentiality of, such information and documents (to the extent that the information and documents will not be kept in compliance with section 187A (and sections 187BA and 187C)); and
 - (c) the day by which the service provider will comply with section 187A (and sections 187BA and 187C) in relation to all such information and documents, except to the extent that any decisions under Division 3 apply.
- (3) The day specified under paragraph (2)(c) must not be later than the day on which the plan would, if approved, cease to be in force under section 187H in relation to the service.

- (4) The plan must also specify:
- (a) any relevant services, operated by the service provider, that the plan does not cover; and
 - (b) the contact details of the officers or employees of the service provider in relation to the plan.

187F Approval of data retention implementation plans

- (1) If, under section 187E, a service provider applies for approval of a data retention implementation plan, the Communications Access Co-ordinator must:
- (a) approve the plan and notify the service provider of the approval; or
 - (b) give the plan back to the service provider with a written request for the service provider to amend the plan to take account of specified matters.
- (2) Before making a decision under subsection (1), the Communications Access Co-ordinator must take into account:
- (a) the desirability of achieving substantial compliance with section 187A (and sections 187BA and 187C) as soon as practicable; and
 - (b) the extent to which the plan would reduce the regulatory burden imposed on the service provider by this Part; and
 - (c) if, at the time the Co-ordinator receives the application, the service provider is contravening section 187A (or section 187BA or 187C) in relation to one or more services covered by the application—the reasons for the contravention; and
 - (d) the interests of law enforcement and national security; and
 - (e) the objects of the *Telecommunications Act 1997*; and
 - (f) any other matter that the Co-ordinator considers relevant.
- (3) If the Communications Access Co-ordinator does not, within 60 days after the day the Co-ordinator receives the application:
- (a) make a decision on the application, and
 - (b) communicate to the applicant the decision on the application;

Section 187G

the Co-ordinator is taken, at the end of that period of 60 days, to have made the decision that the service provider applied for, and to have notified the service provider accordingly.

- (4) A decision that is taken under subsection (3) to have been made in relation to a service provider that applied for the decision has effect only until the Communications Access Co-ordinator makes, and communicates to the service provider, a decision on the application.

187G Consultation with agencies and the ACMA

- (1) As soon as practicable after receiving an application under section 187E to approve a data retention implementation plan (the **original plan**), the Communications Access Co-ordinator must:
- (a) give a copy of the plan to the enforcement agencies and security authorities that, in the opinion of the Co-ordinator, are likely to be interested in the plan; and
 - (b) invite each such enforcement agency or security authority to provide comments on the plan to the Co-ordinator.

The Co-ordinator may give a copy of the plan to the ACMA.

Request for amendment of original plan

- (2) If:
- (a) the Communications Access Co-ordinator receives a comment from an enforcement agency or security authority requesting an amendment of the original plan; and
 - (b) the Co-ordinator considers the request to be a reasonable one;
- the Co-ordinator:
- (c) must request that the service provider make the amendment within 30 days (the **response period**) after receiving the comment or summary; and
 - (d) may give the service provider a copy of the comment or a summary of the comment.

Response to request for amendment of original plan

- (3) The service provider must respond to a request for an amendment of the original plan either:
- (a) by indicating its acceptance of the request, by amending the original plan appropriately and by giving the amended plan to the Communications Access Co-ordinator within the response period; or
 - (b) by indicating that it does not accept the request and providing its reasons for that non-acceptance.

The ACMA's role

- (4) If the service provider indicates that it does not accept a request for an amendment of the original plan, the Communications Access Co-ordinator must:
- (a) refer the request and the service provider's response to the ACMA; and
 - (b) request the ACMA to determine whether any amendment of the original plan is required.
- (5) The ACMA must then:
- (a) determine in writing that no amendment of the original plan is required in response to the request for the amendment; or
 - (b) if, in the opinion of the ACMA:
 - (i) the request for the amendment is a reasonable one; and
 - (ii) the service provider's response to the request for the amendment is not reasonable;determine in writing that the original plan should be amended in a specified manner and give a copy of the determination to the service provider.

Co-ordinator to approve amended plan or to refuse approval

- (6) The Communications Access Co-ordinator must:
- (a) if, on receipt of a determination under paragraph (5)(b), the service provider amends the original plan to take account of that determination and gives the amended plan to the

Section 187H

- Communications Access Co-ordinator—approve the plan as amended, and notify the service provider of the approval; or
- (b) otherwise—refuse to approve the plan, and notify the service provider of the refusal.

ACMA determination not a legislative instrument

- (7) A determination made under subsection (5) is not a legislative instrument.

187H When data retention implementation plans are in force

- (1) A data retention implementation plan for a relevant service operated by a service provider:
- (a) comes into force when the Communications Access Co-ordinator notifies the service provider of the approval of the plan; and
- (b) ceases to be in force in relation to that service:
- (i) if the service provider was operating the service at the commencement of this Part—at the end of the implementation phase for this Part; or
- (ii) if the service provider was not operating the service at the commencement of this Part—at the end of the period of 18 months starting on the day the service provider started to operate the service after that commencement.
- (2) The *implementation phase* for this Part is the period of 18 months starting on the commencement of this Part.

187J Amending data retention implementation plans

- (1) If a service provider's data retention implementation plan is in force, it may be amended only if:
- (a) the service provider applies to the Communications Access Co-ordinator for approval of the amendment, and the Co-ordinator approves the amendment; or

- (b) the Co-ordinator makes a request to the service provider for the amendment to be made, and the service provider agrees to the amendment.
- (2) Section 187F applies in relation to approval of the amendment under paragraph (1)(a) as if the application for approval of the amendment were an application under section 187E for approval of a data retention implementation plan.
- (3) An amendment of a data retention implementation plan:
 - (a) comes into force when:
 - (i) if paragraph (1)(a) applies—the Co-ordinator notifies the service provider of the approval of the amendment; or
 - (ii) if paragraph (1)(b) applies—the service provider notifies the Co-ordinator of the service provider’s agreement to the amendment; but
 - (b) does not effect when the plan ceases to be in force under paragraph 187H(1)(b).

Division 3—Exemptions

187K The Communications Access Co-ordinator may grant exemptions or variations

Decision to exempt or vary

- (1) The Communications Access Co-ordinator may:
 - (a) exempt a specified service provider from the obligations imposed on the service provider under this Part, either generally or in so far as they relate to a specified kind of relevant service; or
 - (b) vary the obligations imposed on a specified service provider under this Part, either generally or in so far as they relate to a specified kind of relevant service; or
 - (c) vary, in relation to a specified service provider, a period specified in section 187C, either generally or in relation to information or documents that relate to a specified kind of relevant service.

A variation must not impose obligations that would exceed the obligations to which a service provider would otherwise be subject under sections 187A and 187C.

- (2) The decision must be in writing.
- (3) The decision may be:
 - (a) unconditional; or
 - (b) subject to such conditions as are specified in the decision.
- (4) A decision made under subsection (1) is not a legislative instrument.

Effect of applying for exemption or variation

- (5) If a service provider applies in writing to the Communications Access Co-ordinator for a particular decision under subsection (1) relating to the service provider:

- (a) the Co-ordinator:
 - (i) must give a copy of the application to the enforcement agencies and security authorities that, in the opinion of the Co-ordinator, are likely to be interested in the application; and
 - (ii) may give a copy of the application to the ACMA; and
- (b) if the Co-ordinator does not, within 60 days after the day the Co-ordinator receives the application:
 - (i) make a decision on the application, and
 - (ii) communicate to the applicant the decision on the application;

the Co-ordinator is taken, at the end of that period of 60 days, to have made the decision that the service provider applied for.
- (6) A decision that is taken under paragraph (5)(b) to have been made in relation to a service provider that applied for the decision has effect only until the Communications Access Co-ordinator makes, and communicates to the service provider, a decision on the application.

Matters to be taken into account

- (7) Before making a decision under subsection (1) in relation to a service provider, the Communications Access Co-ordinator must take into account:
 - (a) the interests of law enforcement and national security; and
 - (b) the objects of the *Telecommunications Act 1997*; and
 - (c) the service provider's history of compliance with this Part; and
 - (d) the service provider's costs, or anticipated costs, of complying with this Part; and
 - (e) any alternative data retention or information security arrangements that the service provider has identified.
- (8) The Communications Access Co-ordinator may take into account any other matter he or she considers relevant.

Section 187KA

187KA Review of exemption or variation decisions

- (1) A service provider may apply in writing to the ACMA for review of a decision under subsection 187K(1) relating to the service provider.
- (2) The ACMA must:
 - (a) confirm the decision; or
 - (b) substitute for that decision another decision that could have been made under subsection 187K(1).

A substituted decision under paragraph (b) has effect (other than for the purposes of this section) as if it were a decision of the Communications Access Co-ordinator under subsection 187K(1).

- (3) Before considering its review of the decision under subsection 187K(1), the ACMA must give a copy of the application to:
 - (a) the Communications Access Co-ordinator; and
 - (b) any enforcement agencies and security authorities that were given, under subparagraph 187K(5)(a)(i), a copy of the application for the decision under review; and
 - (c) any other enforcement agencies and security authorities that, in the opinion of the ACMA, are likely to be interested in the application.

Matters to be taken into account

- (4) Before making a decision under subsection (2) in relation to a service provider, the ACMA must take into account:
 - (a) the interests of law enforcement and national security; and
 - (b) the objects of the *Telecommunications Act 1997*; and
 - (c) the service provider's history of compliance with this Part; and
 - (d) the service provider's costs, or anticipated costs, of complying with this Part; and
 - (e) any alternative data retention or information security arrangements that the service provider has identified.

- (5) The ACMA may take into account any other matter it considers relevant.

Division 4—Miscellaneous

187KB Commonwealth may make a grant of financial assistance to service providers

- (1) The Commonwealth may make a grant of financial assistance to a service provider for the purpose of assisting the service provider to comply with the service provider's obligations under this Part.
- (2) The terms and conditions on which that financial assistance is granted are to be set out in a written agreement between the Commonwealth and the service provider.
- (3) An agreement under subsection (2) may be entered into on behalf of the Commonwealth by the Minister.

187L Confidentiality of applications

- (1) If the Communications Access Co-ordinator receives a service provider's application under section 187E for approval of a data retention implementation plan, or application for a decision under subsection 187K(1), the Co-ordinator must:
 - (a) treat the application as confidential; and
 - (b) ensure that it is not disclosed to any other person or body (other than the ACMA, an enforcement agency or a security authority) without the written permission of the service provider.
- (1A) If the ACMA receives a service provider's application under section 187KA for review of a decision under subsection 187K(1), the ACMA must:
 - (a) treat the application as confidential; and
 - (b) ensure that it is not disclosed to any other person or body (other than the Communications Access Co-ordinator, an enforcement agency or a security authority) without the written permission of the service provider.

Section 187LA

- (2) The ACMA, the Communications Access Co-ordinator, an enforcement agency or a security authority must, if it receives under subsection 187G(1), paragraph 187K(5)(a) or subsection 187KA(3) a copy of a service provider's application:
 - (a) treat the copy as confidential; and
 - (b) ensure that it is not disclosed to any other person or body without the written permission of the service provider.

187LA Application of the *Privacy Act 1988*

- (1) The *Privacy Act 1988* applies in relation to a service provider, as if the service provider were an organisation within the meaning of that Act, to the extent that the activities of the service provider relate to retained data.
- (2) Information that is kept under this Part, or information that is in a document kept under this Part is taken, for the purposes of the *Privacy Act 1988*, to be personal information about an individual if the information relates to:
 - (a) the individual; or
 - (b) a communication to which the individual is a party.

187M Pecuniary penalties and infringement notices

Subsection 187A(1) and paragraph 187D(a) are civil penalty provisions for the purposes of the *Telecommunications Act 1997*.

Note: Parts 31 and 31B of the *Telecommunications Act 1997* provide for pecuniary penalties and infringement notices for contraventions of civil penalty provisions.

187N Review of operation of this Part

- (1) The Parliamentary Joint Committee on Intelligence and Security must review the operation of this Part.
- (1A) The review:
 - (a) must start on or before the second anniversary of the end of the implementation phase; and

Section 187P

- (b) must be concluded on or before the third anniversary of the end of the implementation phase.
- (2) The Committee must give the Minister a written report of the review.
- (3) Until the review is completed, the head (however described) of an enforcement agency must keep:
- (a) all of the documents that he or she is required to retain under section 185; and
 - (b) all of the information that he or she is required, by paragraphs 186(1)(e) to (k), to include in a report under subsection 186(1);
- relating to the period starting on the commencement of this Part and ending when the review is completed.
- (4) Until the review is completed, the Director-General of Security must keep:
- (a) all of the authorisations made under Division 3 of Part 4-1; and
 - (b) all of the information that he or she is required, by paragraphs 94(2A)(c) to (j) of the *Australian Security Intelligence Organisation Act 1979*, to include in a report referred to in subsection 94(1) of that Act;
- relating to the period starting on the commencement of this Part and ending when the review is completed.
- (5) Subsections (3) and (4) do not limit any other obligation to keep information under this Act or another law.

187P Annual reports

- (1) The Minister must, as soon as practicable after each 30 June, cause to be prepared a written report on the operation of this Part during the year ending on that 30 June.
- (1A) Without limiting the matters that may be included in a report under subsection (1), it must include information about:

Section 187P

- (a) the costs to service providers of complying with this Part;
and
 - (b) the use of data retention implementation plans approved
under Division 2 of this Part.
- (2) A report under subsection (1) must be included in the report prepared under subsection 186(2) relating to the year ending on that 30 June.
- (3) A report under subsection (1) must not be made in a manner that is likely to enable the identification of a person.

Part 5-2—Delivery points

188 Delivery points

- (1) Each carrier must:
 - (a) nominate, in respect of a particular kind of telecommunications service of that carrier and in respect of each interception agency, at least one place in Australia as the location of a point from which lawfully intercepted information can most conveniently be transmitted in relation to that interception agency; and
 - (b) inform the Communications Access Co-ordinator of the place or places nominated for each interception agency.

Note 1: The nominated location becomes a delivery point: see the definition of *delivery point* in subsection 5(1).

Note 2: The definition of *carrier* in subsection 5(1) includes carriage service providers.

Note 3: Delivery points are significant for the interception capability obligations in Part 5-3 and for the delivery capability obligations in Part 5-5.

Disagreement over delivery points

- (2) The Communications Access Co-ordinator may, at any time, notify a carrier that an interception agency does not agree to the location of a point nominated under subsection (1) by that carrier in respect of a particular kind of telecommunications service and of that interception agency.
- (3) Upon being so notified, the carrier must nominate another location of a point in respect of that kind of telecommunications service and of that interception agency and inform the Communications Access Co-ordinator.

Note: The nominated location becomes a delivery point: see the definition of *delivery point* in subsection 5(1).

- (4) If the location of a point nominated under subsection (3) is still unsatisfactory to the interception agency, the Communications Access Co-ordinator must:
- (a) inform the carrier to that effect; and
 - (b) refer the disagreement to the ACMA for a determination under subsection (5).
- (5) The ACMA, after hearing the views of the carrier and the views of the interception agency concerning the best location of a point in relation to that kind of telecommunications service and that interception agency, must determine the location of a point for the purposes of this section.

Note: The determined location becomes a delivery point: see the definition of *delivery point* in subsection 5(1).

Factors to be considered in determining delivery points

- (6) In determining the location of a delivery point, the carrier and the interception agency or, failing agreement, the ACMA, must have regard to:
- (a) the configuration of the kind of telecommunications service in respect of which the delivery point is required to be decided; and
 - (b) the relative costs to the carrier and the interception agency of any particular point that is chosen as that delivery point; and
 - (c) the reasonable needs of the interception agency; and
 - (d) the reasonable commercial requirements of the carrier; and
 - (e) the location of any delivery points already existing in relation to that interception agency or other interception agencies.
- (7) It is not a requirement that a place where an interception takes place is the place nominated as the location of a delivery point if, in accordance with the criteria set out in subsection (6), another more suitable location exists.

Changing delivery points

- (8) If:
-

Section 188

- (a) the location of a delivery point has been determined by the ACMA in respect of a particular kind of telecommunications service and of an interception agency; and
- (b) as a result of a material change in the circumstances of the carrier concerned, the location of that point becomes unsuitable;

the carrier:

- (c) may nominate another place as the location of that delivery point in respect of that kind of telecommunications service and of that interception agency; and
- (d) must inform the Communications Access Co-ordinator of the place so nominated.

Note: The nominated location becomes a delivery point: see the definition of *delivery point* in subsection 5(1).

(9) If:

- (a) the location of a delivery point has been determined by the ACMA in respect of a particular kind of telecommunications service and of an interception agency; and
- (b) as a result of a material change in the circumstances of the interception agency, the location of that point becomes unsuitable; and
- (c) the interception agency, either directly or through the Communications Access Co-ordinator, requests the carrier to nominate another place as the location of that delivery point;

the carrier must:

- (d) nominate another place as the location of that delivery point in respect of that kind of telecommunications service and of that interception agency; and
- (e) inform the Communications Access Co-ordinator of the place nominated.

Note: The nominated location becomes a delivery point: see the definition of *delivery point* in subsection 5(1).

(10) Subsections (2) to (7) apply in relation to a nomination under subsection (8) or (9) as if it were a nomination under subsection (1).

Part 5-3—Interception capability

Division 1—Obligations

189 Minister may make determinations

- (1) The Minister may, by legislative instrument, make determinations in relation to interception capabilities applicable to a specified kind of telecommunications service that involves, or will involve, the use of a telecommunications system.
- (2) A determination:
 - (a) must specify an international standard or guidelines (the *international standard*), or the relevant part of the international standard, on which the determination is based; and
 - (b) must provide for interception capability by adopting, applying or incorporating the whole or a part of the international standard, with only such modifications as are necessary to facilitate the application of the standard or the relevant part of the standard in Australia (including any transitional arrangement in relation to an existing kind of telecommunications service that might be required); and
 - (c) must be accompanied by a copy of the international standard or of the relevant part of the international standard.
- (3) For the purposes of subsection (2), the international standard specified in a determination:
 - (a) must deal primarily with the requirements of interception agencies in relation to the interception of communications passing over a telecommunications network and related matters; and
 - (b) may be a part of an international agreement or arrangement or a proposed international agreement or arrangement.

Section 190

Matters to be taken into account

- (4) Before making a determination under subsection (1), the Minister must take into account:
 - (a) the interests of law enforcement and national security; and
 - (b) the objects of the *Telecommunications Act 1997*; and
 - (c) the privacy of the users of telecommunications systems.
- (5) The Minister may take into account any other matter the Minister considers relevant.

190 Obligations of persons covered by a determination

- (1) If a determination under section 189 applies to a particular kind of telecommunications service that involves, or will involve, the use of a telecommunications system, each carrier supplying that kind of service must comply with the determination.

Note: The definition of *carrier* in subsection 5(1) includes carriage service providers.

- (2) Without limiting subsection (1), if a carrier is required to have interception capability in relation to a particular kind of telecommunications service under the determination, the carrier is required to ensure that the capability is developed, installed and maintained.

Note 1: A person may be exempted from the requirements of this section under a provision of Division 2.

Note 2: The cost of this capability is to be borne by the carriers: see Division 2 of Part 5-6.

191 Obligations of persons not covered by a determination in relation to a kind of telecommunications service

- (1) Each carrier supplying a particular kind of telecommunications service that is not covered by any determination under section 189 but that involves, or will involve, the use of a telecommunications system must ensure that the kind of service or the system has the capability to:

Section 191

- (a) enable a communication passing over the system to be intercepted in accordance with an interception warrant; and
- (b) transmit lawfully intercepted information to the delivery points applicable in respect of that kind of service.

Note: The definition of *carrier* in subsection 5(1) includes carriage service providers.

- (2) Without limiting subsection (1), the obligation under that subsection includes the obligation to ensure that the capability is developed, installed and maintained.

Note 1: A person may be exempted from the requirements of this section under a provision of Division 2.

Note 2: The cost of this capability is to be borne by the carriers: see Division 2 of Part 5-6.

Division 2—Exemptions

192 The Communications Access Co-ordinator may grant exemptions

- (1) The Communications Access Co-ordinator may exempt a specified person from all or any of the obligations imposed on the person under Division 1 in so far as those obligations relate to a specified kind of telecommunications service.
- (2) The exemption must be in writing.
- (3) The exemption may be:
 - (a) unconditional; or
 - (b) subject to such conditions as are specified in the exemption.
- (4) An exemption given under subsection (1) is not a legislative instrument.
- (5) If:
 - (a) a person applies in writing to the Communications Access Co-ordinator for an exemption under subsection (1) from all the obligations, or from particular obligations, imposed on the person under Division 1 in so far as those obligations relate to a specified kind of telecommunications service; and
 - (b) the Co-ordinator does not make, and communicate to the applicant, a decision granting, or refusing to grant, the exemption within 60 days after the day on which the Co-ordinator receives the application;the Co-ordinator is taken, at the end of that period of 60 days, to have granted an exemption to the applicant from the obligations to which the application relates in so far as those obligations relate to that kind of telecommunications service.
- (6) An exemption that is taken under subsection (5) to have been granted to a person who applied for an exemption under subsection (1) has effect only until the Communications Access

Co-ordinator makes, and communicates to the person, a decision on the application.

Matters to be taken into account

- (7) Before giving an exemption under subsection (1), the Communications Access Co-ordinator must take into account:
 - (a) the interests of law enforcement and national security; and
 - (b) the objects of the *Telecommunications Act 1997*.
- (8) The Communications Access Co-ordinator may take into account any other matter he or she considers relevant.

193 ACMA may grant exemptions for trial services

- (1) The ACMA may exempt a specified person from all or any of the obligations imposed on the person under Division 1 in so far as those obligations relate to a kind of telecommunications service that is a trial service.
- (2) The ACMA must not grant an exemption unless the ACMA, after consulting any interception agencies that the ACMA considers appropriate, is satisfied that the exemption is unlikely to create a risk to national security or law enforcement.
- (3) The exemption must be in writing.
- (4) The exemption may be:
 - (a) unconditional; or
 - (b) subject to such conditions as are specified in the exemption.
- (5) An exemption given under subsection (1) is not a legislative instrument.

Part 5-4—Interception capability plans

195 Nature of an interception capability plan

- (1) An interception capability plan (*IC plan*) of a carrier or nominated carriage service provider is a written instrument that complies with subsections (2) and (3).

Matters to be included in the instrument

- (2) The instrument must set out:
- (a) a statement of the policies of the carrier or provider in relation to interception generally and of its strategies for compliance with its legal obligation to provide interception capabilities in relation to a particular kind of telecommunications service that involves, or will involve, the use of a telecommunications system; and
 - (b) a statement of the compliance by the carrier or provider with that legal obligation; and
 - (c) a statement of any relevant developments in the business of the carrier or provider that are proposed within the period of 5 years from the start of the plan and that, if implemented, are likely to affect those interception capabilities; and
 - (d) a statement of the locations at which communications passing over a telecommunications system are intercepted or proposed to be intercepted by the carrier or provider; and
 - (e) a list of employees of the carrier or provider with responsibility for interception and other related matters; and
 - (f) the matters determined by the Minister under subsection (4).

Approval of instrument

- (3) The instrument must be approved by the chief executive officer (however described) of the carrier or provider or by a person authorised in writing by that officer for the purposes of this subsection to approve the instrument.

Ministerial determination

- (4) The Minister may, by legislative instrument, determine matters for the purposes of paragraph (2)(f).
- (5) The Minister must consult the ACMA before making a determination under subsection (4).

IC plans are not legislative instruments

- (6) An instrument made under subsection (1) is not a legislative instrument.

196 Time for giving IC plans by carriers

- (1) A carrier must give an IC plan to the Communications Access Co-ordinator by:
 - (a) each 1 July; or
 - (b) if the Co-ordinator agrees to a later day instead of a particular 1 July—that later day.

Note: If the business plans of the carrier change, the carrier may be required to give the Co-ordinator another IC plan under section 201.

- (2) The Communications Access Co-ordinator must inform the ACMA of any agreement under paragraph (1)(b).

Further rule for future carriers

- (3) If the carrier became a carrier on a day (the **start day**) after the commencement of this section, the carrier must also give an IC plan to the Communications Access Co-ordinator within 90 days after the start day.

197 Time for giving IC plans by nominated carriage service providers

- (1) A nominated carriage service provider must give an IC plan to the Communications Access Co-ordinator by:
 - (a) each 1 July; or

Section 198

- (b) if the Co-ordinator agrees to a later day instead of a particular 1 July—that later day.

Note: If the business plans of the nominated carriage service provider change, the provider may be required to give the Co-ordinator another IC plan under section 201.

- (2) The Communications Access Co-ordinator must inform the ACMA of any agreement under paragraph (1)(b).

Further rule for future nominated carriage service providers

- (3) If the carriage service provider became a nominated carriage service provider on a day (the *start day*) after the commencement of this section, the provider must also give an IC plan to the Communications Access Co-ordinator within 90 days after the start day.

Ministerial declaration

- (4) For the purposes of this Part and Part 5-4A, the Minister may, by writing, declare a carriage service provider to be a nominated carriage service provider.
- (5) A declaration made under subsection (4) is not a legislative instrument.

198 Consideration of IC plans

- (1) If a carrier or a nominated carriage service provider gives the Communications Access Co-ordinator an IC plan under section 196, 197 or 201, or an amended IC plan under this section, the Co-ordinator must, within 60 days of receiving the plan:
- (a) approve the plan and notify the carrier or provider of the approval; or
 - (b) give the plan back to the carrier or provider with a written request for the carrier or provider to give the Co-ordinator an amended IC plan to take account of specified matters.

Consultation with interception agencies and the ACMA

- (2) As soon as practicable after receiving an IC plan (the **original plan**) under section 196, 197 or 201, the Communications Access Co-ordinator must:
- (a) give a copy of the plan to:
 - (i) the interception agencies that, in the opinion of the Co-ordinator, are likely to be interested in the plan; and
 - (ii) the ACMA; and
 - (b) invite each such interception agency to provide comments on the plan to the Co-ordinator.

Request for amendment of original plan

- (3) If:
- (a) the Communications Access Co-ordinator receives a comment from an interception agency requesting an amendment of the original plan; and
 - (b) the Co-ordinator considers the request to be a reasonable one; the Co-ordinator must:
 - (c) give the carrier or provider a copy of the comment or a summary of the comment; and
 - (d) request that the carrier or provider respond to the comment or summary within the period (the **response period**) of 30 days of receiving the comment or summary.

Response to request for amendment of original plan

- (4) The carrier or provider must respond to a request for an amendment of the original plan either:
- (a) by indicating its acceptance of the request, by amending the original plan appropriately and by giving the amended plan to the Communications Access Co-ordinator within the response period; or
 - (b) by indicating that it does not accept the request and providing its reasons for that non-acceptance.

Section 199

The ACMA's role

- (5) If the carrier or provider indicates that it does not accept a request for an amendment of the original plan, the Communications Access Co-ordinator must:
- (a) refer the request and the carrier's or provider's response to the ACMA; and
 - (b) request the ACMA to determine whether any amendment of the original plan is required.
- (6) The ACMA must then:
- (a) determine in writing that no amendment of the original plan is required in response to the request for the amendment; or
 - (b) if, in the opinion of the ACMA:
 - (i) the request for the amendment is a reasonable one; and
 - (ii) the carrier's or provider's response to the request for the amendment is not reasonable;determine in writing that the original plan should be amended in a specified manner and give a copy of the determination to the carrier or provider.

Amendment of original plan

- (7) On receipt of a determination under paragraph (6)(b), the carrier or provider must:
- (a) amend the original plan to take account of that determination; and
 - (b) give the amended plan to the Communications Access Co-ordinator.

ACMA determination not a legislative instrument

- (8) A determination made under subsection (6) is not a legislative instrument.

199 Commencement of IC plans

An IC plan of a carrier or nominated carriage service provider:

- (a) comes into force on the day the carrier or provider is notified by the Communications Access Co-ordinator that the plan has been approved; and
- (b) continues in force until the day the carrier or provider is notified by the Co-ordinator that another IC plan of the carrier or provider has been approved.

200 Compliance with IC plans

During the period that an IC plan of a carrier or nominated carriage service provider is in force, the carrier or provider must ensure that its business activities are consistent with the plan.

201 Consequences of changed business plans

- (1) If, because of changes to the business plans of a carrier or nominated carriage service provider, an IC plan given by that carrier or provider ceases, during the period before another such IC plan is due to be given, to constitute an adequate IC plan of that carrier or provider, the carrier or provider must:
 - (a) prepare a new IC plan having regard to those changed business plans; and
 - (b) give the new IC plan to the Communications Access Co-ordinator as soon as practicable.

Note: The new IC plan is subject to consideration in accordance with section 198.

- (2) Subsection (1) applies only if the change in business plans has, or is likely to have, a material adverse effect on the ability of the carrier or provider to comply with its obligations under Part 5-3.

202 Confidential treatment of IC plans

Once the Communications Access Co-ordinator, the ACMA or an interception agency receives an IC plan of a carrier or nominated carriage service provider, the Co-ordinator, the ACMA or the interception agency:

- (a) must treat the plan as confidential; and

Section 202

- (b) must ensure that it is not disclosed to any person or body not referred to in this section without the written permission of the carrier or provider.

Part 5-4A—Requirement arising from proposed changes

202A Purpose of Part

The purpose of this Part is:

- (a) to require carriers and nominated carriage service providers to give notice of the particulars of any change that is proposed in relation to a telecommunications service or a telecommunications system, whose implementation may affect the capacity of the carrier or provider to comply with its obligations under:
 - (i) this Act; or
 - (ii) section 313 of the *Telecommunications Act 1997* (other than subsection 313(1A) or (2A) of that Act); and
- (b) to allow the Communications Access Co-ordinator to notify agencies of such proposed changes.

202B Carrier or provider to notify of proposed change

- (1) This section applies if, at any time, a carrier or a nominated carriage service provider becomes aware that the implementation by the carrier or provider of a change that is proposed to a telecommunications service or a telecommunications system is likely to have a material adverse effect on the capacity of the carrier or provider to comply with its obligations under:
 - (a) this Act; or
 - (b) section 313 of the *Telecommunications Act 1997* (other than subsection 313(1A) or (2A) of that Act).
- (2) A change to a telecommunications service or a telecommunications system includes (but is not limited to) the following:
 - (a) the carrier or carriage service provider providing one or more new telecommunication services;

Section 202B

- (b) the carrier or carriage service provider changing the location of notifiable equipment (including moving equipment outside Australia);
 - (c) the carrier or carriage service provider procuring notifiable equipment (including procuring equipment that is located outside Australia);
 - (d) the carrier or carriage service provider entering into outsourcing arrangements:
 - (i) to have all or part of the telecommunication services provided for the carrier or provider; or
 - (ii) to have all or part of the provision of telecommunication services managed for the carrier or provider; or
 - (iii) to have all or some information to which section 276 of the *Telecommunications Act 1997* applies in relation to the carrier or provider, managed for the carrier or provider;
 - (e) the carrier or carriage service provider entering into arrangements to have all or some information to which section 276 of the *Telecommunications Act 1997* applies in relation to the carrier or provider accessed by persons outside Australia.
- (3) The carrier or provider must notify the Communications Access Co-ordinator, in writing, of its intention to implement the proposed change.
- (4) A notification provided under subsection (3) must include a description of the proposed change.
- (5) After notifying the Communications Access Co-ordinator of a proposed change, the carrier or provider may implement the change if the carrier or provider has not been notified in writing by the Co-ordinator within 30 days after the day the carrier or provider notifies the Co-ordinator.

- (6) If:
- (a) the Communications Access Co-ordinator notifies the carrier or provider in writing within 30 days after the day the carrier or provider notifies the Co-ordinator; and
 - (b) within 30 days after the Co-ordinator so notifies the carrier or provider, the Co-ordinator makes a determination under section 203 that applies to the carrier or provider;
- the carrier or provider must not implement the proposed change until the carrier or provider has complied with the determination.
- (7) To avoid doubt, subsection (6) does not prevent the Communications Access Co-ordinator from making a determination under section 203, that applies to the carrier or provider, more than 30 days after the Co-ordinator first notifies the carrier or provider in writing as mentioned in paragraph (6)(a).

202C Communications Access Co-ordinator may notify agencies

- (1) After the Communications Access Co-ordinator has been notified by a carrier or nominated carriage service provider of an intention to implement a proposed change, the Co-ordinator may notify agencies that are likely to be interested of the proposed change.
- (2) On receiving notification from a carrier or provider of an intention to implement a proposed change, the Communications Access Co-ordinator, and each agency that receives notification of the proposed change, must treat the proposed change as confidential.

Part 5-5—Delivery capability

203 Communications Access Co-ordinator may make determinations

- (1) The Communications Access Co-ordinator may, by writing, make determinations in relation to delivery capabilities applicable in relation to:
- (a) a specified kind of telecommunications service that involves, or will involve, the use of a telecommunications system and that is supplied by one or more specified carriers; and
 - (b) one or more specified interception agencies.

Note 1: The definition of *carrier* in subsection 5(1) includes carriage service providers.

Note 2: For specification by class, see subsection 33(3AB) of the *Acts Interpretation Act 1901*.

Note 3: A determination may make different provision with respect to different matters or different classes of matters (see subsection 33(3A) of the *Acts Interpretation Act 1901*).

- (2) A determination under subsection (1) must relate to all or any of the following:
- (a) the format in which lawfully intercepted information is to be delivered to an interception agency from the delivery point in respect of a kind of telecommunications service and of that interception agency;
 - (b) the place to which, and manner in which, that information is to be delivered;
 - (c) any ancillary information that should accompany that information.
- (3) The Communications Access Co-ordinator must consult the ACMA before making a determination under subsection (1).
- (4) A determination made under subsection (1) is not a legislative instrument.

204 Obligations of persons covered by a determination

- (1) If a determination under section 203 applies:
- (a) to a particular kind of telecommunications service that involves, or will involve, the use of a telecommunications system; and
 - (b) to a carrier;
- the carrier must comply with the determination.

Note: The definition of *carrier* in subsection 5(1) includes carriage service providers.

- (2) Without limiting subsection (1), if a carrier is required to have delivery capability in relation to a particular kind of telecommunications service under the determination, the carrier is required to ensure that the capability is developed, installed and maintained.

Note: The cost of this capability is to be borne by the interception agencies: see Division 3 of Part 5-6.

205 Obligations of persons not covered by a determination in relation to a kind of telecommunications service

- (1) Each carrier supplying a particular kind of telecommunications service that is not covered by any determination under section 203 but that involves, or will involve, the use of a telecommunications system must ensure that the kind of service or the system has a delivery capability.

Note: The definition of *carrier* in subsection 5(1) includes carriage service providers.

- (2) Without limiting subsection (1), the obligation under that subsection includes the obligation to ensure that the capability is developed, installed and maintained.

Note: The cost of this capability is to be borne by the interception agencies: see Division 3 of Part 5-6.

Part 5-6—Allocation of costs

Division 1—Outline of Part

206 Outline of Part

- (1) Division 2 provides that the cost of developing, installing and maintaining an interception capability imposed on a carrier under Part 5-3 is to be borne by the carrier.
- (2) Division 3 provides that the cost of developing, installing and maintaining a delivery capability imposed on a carrier under Part 5-5 is to be borne by the interception agencies.

Note: This Part does not deal with the allocation of costs in relation to carriers complying with authorisations under Division 3 or 4 of Part 4-1. Section 314 of the *Telecommunications Act 1997* deals with this matter.

Division 2—Interception capability

207 Costs to be borne by the carriers

The capital and ongoing costs of developing, installing and maintaining a capability imposed on a carrier under section 190 or 191 in respect of a particular kind of telecommunications service are to be borne by the carrier.

Note: The definition of *carrier* in subsection 5(1) includes carriage service providers.

Division 3—Delivery capability

208 Costs to be borne by the interception agencies

The capital and ongoing costs, worked out in accordance with section 209, of developing, installing and maintaining a delivery capability imposed on a carrier under Part 5-5 in respect of a particular kind of telecommunications service are to be borne by the interception agency concerned.

Note: The definition of *carrier* in subsection 5(1) includes carriage service providers.

209 Working out costs of delivery capabilities

- (1) Each carrier who is obliged to ensure the development, installation and maintenance of a delivery capability must ensure that the capability is developed, installed and maintained on such terms and conditions:
 - (a) as are agreed in writing between the carrier and the interception agency concerned; or
 - (b) in the absence of such an agreement—as are determined in writing by the ACMA.
- (2) The terms and conditions on which a carrier is to provide a delivery capability must be consistent with the following principles:
 - (a) the principle that the most cost effective means of ensuring the development, installation and maintenance of that capability is employed;
 - (b) the principle that the carrier is to incur the costs (whether of a capital nature or otherwise) relating to the development, installation and maintenance of that capability;
 - (c) the principle that the carrier may, over time, recover from an interception agency such of those costs as are required, under section 208, to be borne by that interception agency.

Section 209

- (3) Nothing in subsection (2) prevents a carrier from entering into an agreement with more than one interception agency.
- (4) The agreement should also provide that if the working out of the costs to a particular interception agency of developing, installing and maintaining a delivery capability is the subject of a disagreement between the carrier and that interception agency:
 - (a) the interception agency may request the ACMA to arbitrate the matter; and
 - (b) if it does so, those costs are to be as determined by the ACMA.
- (5) The regulations may make provision in relation to the conduct of an arbitration by the ACMA under this section.
- (6) The existence of a cost dispute in relation to a delivery capability does not affect the obligations of the carrier in respect of that capability while that dispute is being resolved.
- (7) If, as a result of the arbitration of a cost dispute between the carrier and an interception agency, the ACMA concludes that a lesser rate of charge would have been available, the carrier:
 - (a) must allow the interception agency credit for any costs already charged to the extent that they were worked out at a rate that exceeds that lesser rate; and
 - (b) must adjust its means of working out future costs; to take account of that conclusion.
- (8) For the purposes of this section, any reference in this section to terms and conditions agreed between a carrier and an interception agency includes a reference to terms and conditions agreed between the carrier and:
 - (a) in the case of an interception agency of a State—the State, on behalf of the interception agency; and
 - (b) in the case of an interception agency of the Commonwealth—the Commonwealth, on behalf of the interception agency.

Section 210

- (9) A determination made under paragraph (1)(b) is not a legislative instrument.

210 Examination of lower cost options

- (1) In undertaking an arbitration under section 209, the ACMA may on its own initiative or at the request of an interception agency, by notice in writing given to a carrier, require the carrier:
- (a) to examine, at the expense of the carrier, the possibility of a lower cost option than the one designated by the carrier for providing a delivery capability; and
 - (b) to report to the ACMA, within a period specified in the notice, on the results of that examination.
- (2) If a carrier receives a notice under subsection (1), the carrier must, within the period specified in the notice:
- (a) carry out the examination concerned; and
 - (b) report in writing to the ACMA on the results of the examination.
- (3) A notice given under subsection (1) is not a legislative instrument.

211 ACMA may require independent audit of costs

- (1) In undertaking an arbitration under section 209, the ACMA may, by notice in writing, require a carrier to arrange for an audit of the costs claimed to have been incurred by the carrier in relation to the provision to an interception agency of a delivery capability.
- (2) Subject to subsection (3), the audit is to be carried out by an auditor selected by the carrier and approved by the ACMA.
- (3) If the auditor selected by a carrier is not approved by the ACMA, the ACMA may require that the audit be carried out by an auditor selected by the ACMA or by the ACMA itself.
- (4) Unless the audit is carried out by the ACMA itself, the ACMA may, in the notice requiring the audit, specify the period within which the auditor is to report to the ACMA.

Section 211

- (5) If a carrier receives a notice under this section, the carrier:
- (a) must co-operate in full with the person or body carrying out the audit; and
 - (b) must bear the costs of the audit.
- (6) A notice given under this section is not a legislative instrument.

Chapter 6—Miscellaneous

Part 6-1—Miscellaneous

298 Protection of persons—control order declared to be void

- (1) If:
 - (a) a warrant was issued on the basis that an interim control order was in force; and
 - (b) a court subsequently declares the interim control order to be void;
a criminal proceeding does not lie against a person in respect of anything done, or omitted to be done, in good faith by the person:
 - (c) in the purported execution of the warrant; or
 - (d) in the purported exercise of a power, or the purported performance of a function or duty, in a case where the purported exercise of the power, or the purported performance of the function or duty, is consequential on the warrant.
- (2) Subsection (1) does not apply to a thing done, or omitted to be done, at a particular time if, at that time, the person knew, or ought reasonably to have known, of the declaration.

299 Dealing with information obtained under a warrant—control order declared to be void

Scope

- (1) This section applies if:
 - (a) a warrant was issued on the basis that an interim control order was in force; and
 - (b) a court subsequently declares the interim control order to be void; and

Section 299A

- (c) before the declaration was made, information was obtained as a result of:
 - (i) the purported execution of the warrant; or
 - (ii) the purported exercise of a power, or the purported performance of a function or duty, in a case where the purported exercise of the power, or the purported performance of the function or duty, is consequential on the warrant.

Dealing

- (2) A person may:
 - (a) communicate the information to another person; or
 - (b) make use of the information; or
 - (c) make a record of the information; or
 - (d) give the information in evidence in a proceeding;if:
 - (e) the person reasonably believes that doing so is necessary to assist in preventing, or reducing the risk, of:
 - (i) the commission of a terrorist act; or
 - (ii) serious harm to a person; or
 - (iii) serious damage to property; or
 - (f) the person does so for one or more purposes connected with a preventative detention order law.

Definition

- (3) In this section:
serious harm has the same meaning as in the *Criminal Code*.

299A Schedule 1

Schedule 1 has effect.

Section 300

300 Regulations

The Governor-General may make regulations, not inconsistent with this Act, prescribing matters:

- (a) required or permitted by this Act to be prescribed; or
- (b) necessary or convenient to be prescribed for carrying out or giving effect to this Act.

Schedule 1—International production orders

Note: See section 299A.

Part 1—Introduction

1 Simplified outline of this Schedule

- This Schedule provides for a scheme to facilitate cooperation in law enforcement matters between Australia and each foreign country that is a party to a designated international agreement.
- The scheme deals with electronic information held by, or under the control of, prescribed communications providers.
- The scheme has the following components:
 - (a) the issue under this Schedule of international production orders that are directed to prescribed communications providers;
 - (b) in a case where a corresponding order is issued by a competent authority of a foreign country in accordance with a designated international agreement—the exemption of acts or things done in compliance with such an order from Commonwealth laws restricting interception or disclosure.
- The scheme extends to matters outside Australia.
- An international production order may be issued for purposes in connection with:
 - (a) the investigation of an offence of a serious nature; or
 - (b) the monitoring of a person subject to a Part 5.3 supervisory order, so as to achieve a Part 5.3 object; or
 - (c) the carrying out by the Organisation of its functions.

Clause 2

- There are 3 types of international production orders:
 - (a) international production orders relating to interception; and
 - (b) international production orders relating to stored communications; and
 - (c) international production orders relating to telecommunications data.

2 Definitions

In this Schedule:

access, when used in relation to material, includes:

- (a) access that is subject to a pre-condition (for example, the use of a password); and
- (b) access by way of push technology; and
- (c) access by way of a standing request.

account includes:

- (a) a free account; and
- (b) a pre-paid account; and
- (c) anything that may reasonably be regarded as the equivalent of an account.

ASIO official means:

- (a) the Director-General of Security; or
- (b) a Deputy Director-General of Security; or
- (c) an ASIO employee; or
- (d) an ASIO affiliate.

Attorney-General's Department means the Department administered by the Attorney-General.

Australian Designated Authority means the Secretary of the Attorney-General's Department.

based in a foreign country has the meaning given by clause 10A.

certified copy:

- (a) in relation to an international production order issued under clause 30—has the meaning given by clause 174; or
- (b) in relation to an international production order issued under clause 39—has the meaning given by clause 175; or
- (c) in relation to an international production order issued under clause 48—has the meaning given by clause 176; or
- (d) in relation to an international production order issued under clause 60—has the meaning given by subclause 177(2); or
- (e) in relation to an international production order issued under clause 69—has the meaning given by subclause 177(4); or
- (f) in relation to an international production order issued under clause 78—has the meaning given by subclause 177(6); or
- (g) in relation to an international production order issued under clause 89—has the meaning given by subclause 178(2); or
- (h) in relation to an international production order issued under clause 98—has the meaning given by subclause 178(4); or
- (i) in relation to an international production order issued under clause 107—has the meaning given by subclause 178(6).

designated international agreement has the meaning given by clause 3.

eligible Judge has the meaning given by clause 14.

eligible position-holder means an ASIO employee, or an ASIO affiliate, who holds, or is acting in, a position in the Organisation that is equivalent to or higher than a position occupied by an Executive Level 2 APS employee.

general electronic content service has the meaning given by clause 8.

general electronic content service provider means a person who provides a general electronic content service to the public or a section of the public.

Clause 2

individual message/call application service means a message/call application service to the extent to which the service is provided using a particular telecommunications identifier.

individual transmission service means a transmission service to the extent to which the service is supplied using a particular telecommunications identifier.

intended recipient of a communication has the meaning given by clause 11.

intercept means:

- (a) record; or
- (b) live stream to a single destination.

international production order means an international production order issued under this Schedule.

issuing authority means a person in respect of whom an appointment is in force under clause 16.

manager of a prescribed communications provider means:

- (a) the chief executive officer (however described) of the provider; or
- (b) any other individual who is involved in the management of the provider.

material means material:

- (a) whether in the form of text; or
- (b) whether in the form of data; or
- (c) whether in the form of speech, music or other sounds; or
- (d) whether in the form of visual images (moving or otherwise);
or
- (e) whether in the form of signals; or
- (f) whether in any other form; or
- (g) whether in any combination of forms.

meets the enforcement threshold has the meaning given by clause 125.

member of staff of the Attorney-General's Department means:

- (a) the Secretary of the Attorney-General's Department; or
- (b) an APS employee in that Department.

message means a message:

- (a) whether in the form of text; or
- (b) whether in the form of data; or
- (c) whether in the form of speech, music or other sounds; or
- (d) whether in the form of visual images (animated or otherwise); or
- (e) whether in the form of signals; or
- (f) whether in any other form; or
- (g) whether in any combination of forms.

message application service has the meaning given by clause 4.

message/call application service means:

- (a) a message application service; or
- (b) a voice call application service; or
- (c) a video call application service.

message/call application service provider means a person who provides a message/call application service to the public or a section of the public.

network entity means a person who owns or operates a telecommunications network that is used to supply a transmission service to the public or a section of the public.

nominated AAT member means a member of the Administrative Appeals Tribunal in respect of whom a nomination is in force under clause 15 to issue international production orders under Division 2 of Part 2, and Division 2 of Part 3, of this Schedule.

nominated AAT Security Division member means a member of the Administrative Appeals Tribunal in respect of whom a nomination is in force under clause 17 to issue international production orders under Part 4 of this Schedule.

Clause 2

operates in a foreign country has the meaning given by clause 10A.

Part 5.3 IPO agency means a Part 5.3 warrant agency to the extent that the agency applies for warrants issued in relation to Part 5.3 supervisory orders in force in relation to persons.

posted on a general electronic content service has the meaning given by clause 9.

prescribed communications provider means:

- (a) a network entity; or
- (b) a transmission service provider; or
- (c) a message/call application service provider; or
- (d) a storage/back-up service provider; or
- (e) a general electronic content service provider.

protected information means:

- (a) information obtained in accordance with an international production order; or
- (b) information about any of the following:
 - (i) an application for an international production order;
 - (ii) the issue of an international production order;
 - (iii) the existence or non-existence of an international production order;
 - (iv) compliance or non-compliance with an international production order;
 - (v) the revocation of an international production order;
 - (vi) the cancellation of an international production order.

relevant agency means:

- (a) an interception agency; or
- (b) a criminal law-enforcement agency; or
- (c) an enforcement agency; or
- (d) a Part 5.3 IPO agency.

relevant statistics, in relation to applications of a particular kind, means the following statistics:

- (a) how many applications of that kind were made;
- (b) how many applications of that kind were withdrawn;
- (c) how many applications of that kind were refused;
- (d) how many international production orders were issued in response to applications of that kind.

senior position-holder has the same meaning as in the *Australian Security Intelligence Organisation Act 1979*.

serious category 1 offence means:

- (a) an offence that is punishable by a maximum term of imprisonment of 3 years or more; or
- (b) an offence that is punishable by imprisonment for life.

Note: For the definition of **offence**, see section 5.

serious category 2 offence means:

- (a) a serious offence (see section 5D); or
- (b) an offence that is punishable by a maximum term of imprisonment of 7 years or more; or
- (c) an offence that is punishable by imprisonment for life.

Note: For the definition of **offence**, see section 5.

service includes a website. This definition does not apply to the definition of **transmission service**.

statutory requirements certificate means a certificate under subclause 3B(2).

storage/back-up service has the meaning given by clause 7.

storage/back-up service provider means a person who provides a storage/back-up service to the public or a section of the public.

stored communication means:

- (a) a communication that:
 - (i) has been carried by a transmission service; and

Clause 2

- (ii) is not being carried by a transmission service; and
 - (iii) is held on equipment that is operated by, and is in the possession of, the transmission service provider who supplied the transmission service; or
- (b) a communication that:
- (i) has been carried by a transmission service; and
 - (ii) is not being carried by a transmission service; and
 - (iii) is held on equipment that is operated by, and is in the possession of, the network entity who owns or operates a telecommunications network used to supply the transmission service; or
- (c) a message that:
- (i) has been sent or received using a message/call application service provided by a message/call application service provider; and
 - (ii) is held on equipment that is operated by, and is in the possession of, the message/call application service provider; or
- (d) a recording of a voice call that:
- (i) has been made or received using a message/call application service provided by a message/call application service provider; and
 - (ii) is held on equipment that is operated by, and is in the possession of, the message/call application service provider; or
- (e) a recording of a video call that:
- (i) has been made or received using a message/call application service provided by a message/call application service provider; and
 - (ii) is held on equipment that is operated by, and is in the possession of, the message/call application service provider; or

- (f) material that:
 - (i) has been uploaded by an end-user for storage or back-up by a storage/back-up service provided by a storage/back-up service provider; and
 - (ii) is held on equipment that is operated by, and is in the possession of, the storage/back-up service provider; or
- (g) material that:
 - (i) is accessible to, or deliverable to, one or more of the end-users using a general electronic content service provided by a general electronic content service provider; and
 - (ii) is held on equipment that is operated by, and is in the possession of, the general electronic content service provider.

telecommunications data:

- (a) when used in relation to a communication carried by an individual transmission service—means information about the communication (other than information that is the contents or substance of the communication); or
- (b) when used in relation to an individual transmission service—means information about the individual transmission service; or
- (c) when used in relation to a message sent or received using an individual message/call application service—means information about the message (other than information that is the contents or substance of the message); or
- (d) when used in relation to a voice call made or received using an individual message/call application service—means information about the voice call (other than information that is the contents or substance of the voice call); or
- (e) when used in relation to a video call made or received using an individual message/call application service—means information about the video call (other than information that is the contents or substance of the video call); or

Clause 2

- (f) when used in relation to an individual message/call application service—means information about the individual message/call application service; or
- (g) when used in relation to material that has been uploaded by an end-user for storage or back-up by a storage/back-up service—means information about the material (other than information that is the content or substance of the material); or
- (h) when used in relation to an account that a person has with a storage/back-up service—means information relating to the account; or
- (i) when used in relation to material that has been posted on a general electronic content service—means information about the material (other than information that is the content or substance of the material); or
- (j) when used in relation to an account that a person has with a general electronic content service—means information relating to the account; or
- (k) when used otherwise than in relation to a matter or thing mentioned in any of the preceding paragraphs—means:
 - (i) information about a communication carried by an individual transmission service (other than information that is the contents or substance of the communication); or
 - (ii) information about an individual transmission service; or
 - (iii) information about a message sent or received using an individual message/call application service (other than information that is the contents or substance of the message); or
 - (iv) information about a voice call made or received using an individual message/call application service (other than information that is the contents or substance of the voice call); or
 - (v) information about a video call made or received using an individual message/call application service (other

- than information that is the contents or substance of the video call); or
- (vi) information about an individual message/call application service; or
 - (vii) information about material that has been uploaded by an end-user for storage or back-up by a storage/back-up service (other than information that is the content or substance of the material); or
 - (viii) information relating to an account that a person has with a storage/back-up service; or
 - (ix) information about material that has been posted on a general electronic content service (other than information that is the content or substance of the material); or
 - (x) information relating to an account that a person has with a general electronic content service.

telecommunications identifier means:

- (a) the address or identifier used by a network entity or a transmission service provider for the purposes of:
 - (i) directing a communication to its intended destination; or
 - (ii) identifying the origin of a communication; or
- (b) the address or identifier used by a message/call application service provider for the purposes of:
 - (i) directing a message to its intended destination; or
 - (ii) identifying the origin of a message; or
- (c) the address or identifier used by a message/call application service provider for the purposes of:
 - (i) directing a voice call to its intended destination; or
 - (ii) identifying the origin of a voice call; or
- (d) the address or identifier used by a message/call application service provider for the purposes of:
 - (i) directing a video call to its intended destination; or
 - (ii) identifying the origin of a video call;

and includes (for example):

Clause 3

- (e) a telephone number; and
- (f) a unique identifier for a device (for example, an electronic serial number or a Media Access Control address); and
- (g) a user account identifier; and
- (h) an internet protocol address; and
- (i) an email address.

telecommunications network means a system, or series of systems, that carries, or is capable of carrying, communications by means of guided and/or unguided electromagnetic energy.

telephone application means an application made by telephone for an international production order.

telephone number includes a mobile telephone number.

transmission service means a service for carrying communications by means of guided and/or unguided electromagnetic energy.

transmission service provider means a person who supplies a transmission service to the public or a section of the public.

uploaded has a meaning affected by clause 10.

urgent circumstances has a meaning affected by clause 17A.

use has a meaning affected by clause 12.

video call includes a video call that has an audio component.

video call application service has the meaning given by clause 6.

voice call includes a call that involves a recorded or synthetic voice.

voice call application service has the meaning given by clause 5.

3 Designated international agreement

Bilateral agreement

- (1) For the purposes of this Schedule, if:
- (a) there is an agreement between Australia and a foreign country; and
 - (b) a copy of the English text of the agreement is set out in the regulations; and
 - (c) the agreement has entered into force for Australia and the foreign country;
- then:
- (d) if the agreement is affected by an amendment, where:
 - (i) a copy of the English text of the amendment is set out in the regulations; and
 - (ii) the amendment has entered into force for Australia and the foreign country;the agreement, as affected by such an amendment, is a ***designated international agreement***; or
 - (e) if paragraph (d) does not apply—the agreement is a ***designated international agreement***.

Note: An agreement mentioned in paragraph (a) is a treaty to which Australia is a party. Proposed treaty actions, such as amendments of treaties and extensions of the duration of treaties, are subject to Australia's treaty-making process. In 2021, the parliamentary scrutiny process for proposed treaty actions included tabling in both Houses of the Parliament and consideration by the Joint Standing Committee on Treaties.

- (1A) If:
- (a) there is an agreement between Australia and a foreign country; and
 - (b) the agreement deals with (among other things) the issue of orders (however described) by a competent authority (however described) of the foreign country;
- a copy of the English text of the agreement must not be set out in regulations made for the purposes of paragraph (1)(b) unless a

Clause 3

statutory requirements certificate is in force under clause 3B in relation to the foreign country and the agreement.

- (2) If:
- (a) there is an agreement between Australia and a foreign country; and
 - (b) the agreement deals with (among other things) the issue of orders (however described) by a competent authority (however described) of the foreign country; and
 - (c) one or more offences against the law of the foreign country are death penalty offences;

a copy of the English text of the agreement must not be set out in regulations made for the purposes of paragraph (1)(b) unless the Minister has received a written assurance from the government of the foreign country, relating to the use or non-use of Australian-sourced information obtained by virtue of the agreement, in connection with any proceeding by way of a prosecution for a death penalty offence in the foreign country. For the purposes of this subclause, information is obtained by virtue of the agreement if it is obtained in accordance with such an order.

Note 1: For *Australian-sourced information*, see subclause (8).

Note 2: For *death penalty offence*, see subclause (7A).

Multilateral agreement

- (3) For the purposes of this Schedule, if:
- (a) there is an agreement between Australia and 2 or more foreign countries; and
 - (b) a copy of the English text of the agreement is set out in the regulations; and
 - (c) the agreement has entered into force for Australia;
- then:
- (d) if the agreement is affected by an amendment, where:
 - (i) a copy of the English text of the amendment is set out in the regulations; and
 - (ii) the amendment has entered into force for Australia;

the agreement, as affected by such an amendment, is a ***designated international agreement***; or

- (e) if paragraph (d) does not apply—the agreement is a ***designated international agreement***.

Note: An agreement mentioned in paragraph (a) is a treaty to which Australia is a party. Proposed treaty actions, such as amendments of treaties and extensions of the duration of treaties, are subject to Australia's treaty-making process. In 2021, the parliamentary scrutiny process for proposed treaty actions included tabling in both Houses of the Parliament and consideration by the Joint Standing Committee on Treaties.

- (4) If there is an agreement between Australia and 2 or more foreign countries, the regulations may declare that one or more of those foreign countries are ***recognised parties*** to the agreement for the purposes of this Schedule.

(4A) If:

- (a) there is an agreement between Australia and 2 or more foreign countries; and
(b) the agreement deals with (among other things) the issue of orders (however described) by a competent authority (however described) of each of the foreign countries;

a foreign country that is a party to the agreement must not be declared under subclause (4) unless a statutory requirements certificate is in force under clause 3B in relation to the foreign country and the agreement.

(5) If:

- (a) there is an agreement between Australia and 2 or more foreign countries; and
(b) the agreement deals with (among other things) the issue of orders (however described) by a competent authority (however described) of each of the foreign countries; and
(c) one or more offences against the law of one or more of those foreign countries are death penalty offences;

a foreign country covered by paragraph (c) must not be declared under subclause (4) unless the Minister has received a written

Clause 3

assurance from the government of the foreign country, relating to the use or non-use of Australian-sourced information obtained by virtue of the agreement, in connection with any proceeding by way of a prosecution for a death penalty offence in the foreign country. For the purposes of this subclause, information is obtained by virtue of the agreement if it is obtained in accordance with such an order.

Note 1: For *Australian-sourced information*, see subclause (8).

Note 2: For *death penalty offence*, see subclause (7A).

- (6) If:
- (a) apart from this subclause, there is a designated international agreement between Australia and one or more foreign countries; and
 - (b) one or more of those foreign countries are not recognised parties to the agreement;
- this Schedule (other than subclauses (3) and (4)) has effect as if those foreign countries were not parties to the agreement.

Note: For *recognised parties*, see subclause (4).

Announcement by Minister

- (7) The Minister must announce, by notifiable instrument, the day an agreement mentioned in subclause (1) or (3) enters into force for Australia.

Death penalty offence

- (7A) For the purposes of this clause, *death penalty offence* means an offence against a law of a foreign country that is punishable by death.

Australian-sourced information

- (8) For the purposes of the application of subclause (2) or (5) to an order, information obtained in accordance with the order is *Australian-sourced information* if the order:
- (a) requires an act or thing to be done in Australia; or

- (b) is directed to an individual who is physically present in Australia; or
- (c) is directed to a body corporate that is incorporated in Australia; or
- (d) is directed to a body established by or under a law of the Commonwealth, a State or a Territory.

3A Disallowance of regulations relating to designated international agreements

Scope

- (1) This clause applies to regulations made for the purposes of clause 3.

Disallowance

- (2) Either House of the Parliament may, following a motion upon notice, pass a resolution disallowing the regulations. For the resolution to be effective:
 - (a) the notice must be given in that House within 15 sitting days of that House after the copy of the regulations was tabled in that House under section 38 of the *Legislation Act 2003*; and
 - (b) the resolution must be passed, in pursuance of the motion, within 15 sitting days of that House after the giving of that notice.
- (3) If neither House passes such a resolution, the regulations takes effect on the day immediately after the last day upon which such a resolution could have been passed if it were assumed that notice of a motion to disallow the regulations was given in each House on the last day of the 15 sitting day period of that House mentioned in paragraph (2)(a).
- (4) If:
 - (a) notice of a motion to disallow the regulations is given in a House of the Parliament within 15 sitting days of that House

Clause 3B

after the copy of the regulations was tabled in that House under section 38 of the *Legislation Act 2003*; and

- (b) at the end of 15 sitting days of that House after the giving of that notice of motion:
- (i) the notice has not been withdrawn and the motion has not been called on; or
 - (ii) the motion has been called on, moved and (where relevant) seconded and has not been withdrawn or otherwise disposed of;

the regulations is then taken to have been disallowed, and subclause (3) does not apply to the regulations.

- (5) Section 42 (disallowance) of the *Legislation Act 2003* does not apply to the regulations.

Note 1: The 15 sitting day notice period mentioned in paragraph (2)(a) of this clause is the same as the 15 sitting day notice period mentioned in paragraph 42(1)(a) of the *Legislation Act 2003*.

Note 2: The 15 sitting day disallowance period mentioned in paragraph (2)(b) of this clause is the same as the 15 sitting day disallowance period mentioned in paragraph 42(1)(b) of the *Legislation Act 2003*.

3B Statutory requirements certificate—designated international agreements

Scope

- (1) This section applies if:
- (a) there is an agreement between Australia and one or more foreign countries; and
 - (b) the agreement deals with (among other things) the issue of orders (however described) by a competent authority (however described) of the foreign country, or each of the foreign countries, concerned.

Certificate

- (2) The Attorney-General may, after consulting the Minister and the Minister for Foreign Affairs, issue a certificate (a **statutory requirements certificate**) in relation to:
- (a) a foreign country that is a party to the agreement; and
 - (b) the agreement.
- (3) A statutory requirements certificate is a notifiable instrument.
- (4) The Attorney-General must not issue a statutory requirements certificate in relation to:
- (a) a foreign country that is a party to the agreement; and
 - (b) the agreement;
- unless the Attorney-General is satisfied that:
- (c) the agreement is appropriate in the circumstances, having regard only to:
 - (i) the foreign country's respect for the rule of law; and
 - (ii) the foreign country's respect for its obligations under international law relating to human rights; and
 - (d) the following requirements are met in relation to orders (however described) issued by a competent authority (however described) of the foreign country:
 - (i) the agreement provides that orders are to be issued in compliance with the law of the foreign country;
 - (ii) the agreement provides that orders may only be issued for the purposes of obtaining information relevant to the prevention, detection, investigation or prosecution of serious crime (as defined in the agreement);
 - (iii) the agreement provides that orders may not be issued for the purposes of investigating, prosecuting or punishing a person on account of the person's political opinions;
 - (iv) the agreement, so far as it relates to orders, is appropriate in the circumstances, having regard only to the matters set out in subclause (5);

Clause 3C

- (v) the agreement does not permit orders to be issued for the purposes of obtaining information about the communications of a person who is an Australian citizen or a permanent resident of Australia;
 - (vi) the agreement provides for limitations and safeguards relating to the use, handling and disclosure of information obtained in accordance with orders;
 - (vii) the agreement does not permit orders to be issued on behalf of another country;
 - (viii) the agreement does not impose obligations on the foreign country to share information it has obtained in accordance with orders with another country; and
- (e) if one or more offences against the law of the foreign country are death penalty offences (within the meaning of clause 3)—the Minister has received a written assurance from the government of the foreign country in accordance with subclause 3(2) or (5).
- (5) For the purposes of subparagraph (4)(d)(iv), the matters are:
- (a) criteria for the issuing of orders; and
 - (b) limitations on the scope and objects of orders; and
 - (c) limits on the periods for which orders are in force;
- set out in the agreement or the law of the foreign country.

Copy of certificate to be given to the Chair of the Joint Standing Committee on Treaties

- (6) If the Attorney-General issues a statutory requirements certificate, the Attorney-General must:
- (a) give a copy of the certificate to the Chair of the Joint Standing Committee on Treaties; and
 - (b) do so as soon as practicable after the certificate is issued.

3C Australia's treaty-making process

Nothing in this Schedule is intended to modify or limit the application of Australia's treaty-making process relating to a

designated international agreement, including the following proposed treaty actions:

- (a) an amendment of a designated international agreement;
- (b) an extension of the duration of a designated international agreement.

4 Message application service

- (1) For the purposes of this Schedule, ***message application service*** means a service that enables end-users to send or receive messages to or from other end-users using a transmission service.
- (2) For the purposes of subclause (1), it is immaterial whether the service also enables end-users to send or receive messages to or from persons (other than end-users) using a transmission service.
Example: A webmail service that enables end-users to send emails to, or receive emails from, any email address.
- (3) For the purposes of this Schedule, a person does not provide a message application service merely because the person supplies a transmission service that enables messages to be sent or received.
- (4) For the purposes of this Schedule, a person does not provide a message application service merely because the person provides a billing service, or a fee collection service, in relation to a message application service.

5 Voice call application service

- (1) For the purposes of this Schedule, ***voice call application service*** means a service that enables end-users to make or receive voice calls to or from other end-users using a transmission service.
- (2) For the purposes of subclause (1), it is immaterial whether the service also enables end-users to make or receive voice calls to or from persons (other than end-users) using a transmission service.
Example: A VOIP service that enables end-users to make voice calls to, or receive voice calls from, any telephone number.

Clause 6

- (3) For the purposes of this Schedule, a person does not provide a voice call application service merely because the person supplies a transmission service that enables voice calls to be made or received.
- (4) For the purposes of this Schedule, a person does not provide a voice call application service merely because the person provides a billing service, or a fee collection service, in relation to a voice call application service.

6 Video call application service

- (1) For the purposes of this Schedule, ***video call application service*** means a service that enables end-users to make or receive video calls to or from other end-users using a transmission service.
- (2) For the purposes of subclause (1), it is immaterial whether the service also enables end-users to make or receive video calls to or from persons (other than end-users) using a transmission service.
- (3) For the purposes of this Schedule, a person does not provide a video call application service merely because the person supplies a transmission service that enables video calls to be made or received.
- (4) For the purposes of this Schedule, a person does not provide a video call application service merely because the person provides a billing service, or a fee collection service, in relation to a video call application service.

7 Storage/back-up service

- (1) For the purposes of this Schedule, ***storage/back-up service*** means a service that enables end-users to store or back-up material, where the uploading of the material for storage or back-up is by means of a transmission service.
- (2) For the purposes of this Schedule, a person does not provide a storage/back-up service merely because the person supplies a

transmission service that enables material to be uploaded for storage or back-up.

- (3) For the purposes of this Schedule, a person does not provide a storage/back-up service merely because the person provides a billing service, or a fee collection service, in relation to a storage/back-up service.

8 General electronic content service

- (1) For the purposes of this Schedule, *general electronic content service* means:
- (a) a service that allows end-users to access material using a transmission service; or
 - (b) a service that delivers material to persons having equipment appropriate for receiving that material, where the delivery of the service is by means of a transmission service;
- but does not include:
- (c) a message/call application service; or
 - (d) a storage/back-up service; or
 - (e) a service prescribed by the regulations.
- (2) For the purposes of this Schedule, a person does not provide a general electronic content service merely because the person supplies a transmission service that enables material to be accessed or delivered.
- (3) For the purposes of this Schedule, a person does not provide a general electronic content service merely because the person provides a billing service, or a fee collection service, in relation to a general electronic content service.

9 When material is posted on a general electronic content service

For the purposes of this Schedule, material is *posted* on a general electronic content service by a person if:

- (a) the person is an end-user of the service; and

Clause 10

- (b) the person causes the material to be accessible to, or delivered to, one or more other end-users using the service.

10 Uploaded material

For the purposes of this Schedule, if:

- (a) a person uses a device; and
 - (b) the device has software that automatically uploads material for storage or back-up by a storage/back-up service; and
 - (c) as a result, material is automatically uploaded for storage or back-up by the storage/back-up service;
- the person is taken to have uploaded the material for storage or back-up by the storage/back-up service.

10A When a prescribed communications provider is based in, or operates in, a foreign country

Based in a foreign country—individual

- (1) For the purposes of the application of this Schedule to a prescribed communications provider who is an individual, the provider is **based in** a foreign country if, and only if, the provider is ordinarily resident in the foreign country.

Based in a foreign country—body corporate

- (2) For the purposes of the application of this Schedule to a prescribed communications provider that is a body corporate, the provider is **based in** a foreign country if, and only if:
 - (a) the provider is incorporated in the foreign country; or
 - (b) the provider has its principal place of business in the foreign country.

Operates in a foreign country

- (3) For the purposes of this Schedule, a prescribed communications provider **operates in** a foreign country if, and only if:

- (a) the provider handles communications in the foreign country;
or
- (b) the provider holds stored communications in the foreign
country; or
- (c) the provider holds telecommunications data in the foreign
country.

11 Intended recipient of a communication

For the purposes of this Schedule, the *intended recipient* of a communication is:

- (a) if the communication is addressed to an individual (either in the individual's own capacity or in the capacity of an employee or agent of another person)—the individual; or
- (b) if the communication is addressed to a person who is not an individual—the person; or
- (c) if the communication is not addressed to a person—the person who has, or whose employee or agent has, control over the individual transmission service that was used to receive the communication.

12 Use of a thing

A reference in this Schedule to the *use* of a thing is a reference to the use of the thing either:

- (a) in isolation; or
- (b) in conjunction with one or more other things.

Note: See also section 18A of the *Acts Interpretation Act 1901*.

13 Identification of a particular person

For the purposes of this Schedule, a particular person may be identified:

- (a) by the person's full name; or
- (b) by a name by which the person is commonly known; or

Clause 14

- (c) as the person to whom a particular individual transmission service is supplied; or
- (d) as the person to whom a particular individual message/call application service is provided; or
- (e) as the person who has a particular account with a prescribed communications provider; or
- (f) as the person who has a particular telephone number; or
- (g) as the person who has a particular email address; or
- (h) as the person who has a particular internet protocol address; or
- (i) as the person who has a device that has a particular unique identifier (for example, an electronic serial number or a Media Access Control address); or
- (j) by any other unique identifying factor that is applicable to the person.

14 Eligible judge

- (1) For the purposes of this Schedule, *eligible Judge* means a Judge in relation to whom a consent under subclause (2) and a declaration under subclause (3) are in force.
- (2) A Judge may, by writing, consent to be nominated by the Attorney-General under subclause (3).
- (3) The Attorney-General may, by writing, declare Judges in relation to whom consents are in force under subclause (2) to be eligible Judges for the purposes of this Schedule.
- (4) An eligible Judge has, in relation to the performance or exercise of a function or power conferred on an eligible Judge by this Schedule, the same protection and immunity as a Justice of the High Court has in relation to proceedings in the High Court.

15 Nominated AAT member

- (1) The Attorney-General may, by writing, nominate a person who holds one of the following appointments to the Administrative

Appeals Tribunal to issue international production orders under Division 2 of Part 2, and Division 2 of Part 3, of this Schedule:

- (a) Deputy President;
 - (b) senior member (of any level);
 - (c) member (of any level).
- (2) Despite subclause (1), the Attorney-General must not nominate a person who holds an appointment as a part-time senior member or a member of the Tribunal unless the person:
- (a) is enrolled as a legal practitioner of the High Court, of another federal court or of the Supreme Court of a State or of the Australian Capital Territory; and
 - (b) has been so enrolled for not less than 5 years.
- (3) A nomination ceases to have effect if the nominated AAT member ceases to hold an appointment of a kind set out in subclause (1).
- (4) A nominated AAT member has, in relation to the performance or exercise of a function or power conferred on a nominated AAT member by this Schedule, the same protection and immunity as a Justice of the High Court has in relation to proceedings in the High Court.

16 Issuing authority

- (1) The Attorney-General may, by writing, appoint as an issuing authority:
- (a) a person who is:
 - (i) a judge of a court created by the Parliament; or
 - (ii) a magistrate;and in relation to whom a consent under subclause (2) is in force; or
 - (b) a person who:
 - (i) holds an appointment to the Administrative Appeals Tribunal as Deputy President, senior member (of any level) or member (of any level); and

Clause 17

- (ii) is enrolled as a legal practitioner of a federal court or of the Supreme Court of a State or a Territory; and
 - (iii) has been so enrolled for at least 5 years.
- (2) A person who is:
- (a) a judge of a court created by the Parliament; or
 - (b) a magistrate;
- may, by writing, consent to be appointed by the Attorney-General under subclause (1).
- (3) A person's appointment ceases to have effect if the person ceases to be a person whom the Attorney-General could appoint under this clause.
- (4) An appointment under subclause (1) has no effect for the purposes of a provision of this Act (other than this Schedule).
- (5) An issuing authority has, in relation to the performance or exercise of a function or power conferred on an issuing authority by this Schedule, the same protection and immunity as a Justice of the High Court has in relation to proceedings in the High Court.

17 Nominated AAT Security Division member

- (1) The Attorney-General may, by writing, nominate a person who:
- (a) holds one of the following appointments to the Administrative Appeals Tribunal:
 - (ii) senior member (of any level);
 - (iii) member (of any level); and
 - (b) is a member of the Security Division of the Administrative Appeals Tribunal;
- to issue international production orders under Part 4 of this Schedule.
- (2) Despite subclause (1), the Attorney-General must not nominate a person who holds an appointment as a part-time senior member or a member of the Administrative Appeals Tribunal unless the person:

Clause 17A

- (a) is enrolled as a legal practitioner of the High Court, of another federal court or of the Supreme Court of a State or of the Australian Capital Territory; and
 - (b) has been so enrolled for not less than 5 years.
- (3) A nomination of a person under subclause (1) ceases to have effect if:
- (a) the person ceases to hold an appointment of a kind set out in subclause (1); or
 - (b) the person ceases to be a member of the Security Division of the Administrative Appeals Tribunal.
- (3A) The Attorney-General may, by writing, nominate a person who is a Deputy President of the Administrative Appeals Tribunal to issue international production orders under Part 4 of this Schedule.
- (3B) A nomination of a person under subclause (3A) ceases to have effect if the person ceases to be a Deputy President of the Administrative Appeals Tribunal.
- (4) A nominated AAT Security Division member has, in relation to the performance or exercise of a function or power conferred on a nominated AAT Security Division member by this Schedule, the same protection and immunity as a Justice of the High Court has in relation to proceedings in the High Court.
- (5) For the purposes of this clause, a person is a ***member of the Security Division of the Administrative Appeals Tribunal*** if the person:
- (a) is the head of that Division; or
 - (b) has been assigned to that Division.

17A Urgent circumstances

- (1) For the purposes of this Schedule, it is necessary, because of urgent circumstances, to make an application under Part 2 or 3 of this Schedule for an international production order by telephone if, and only if:

Clause 18

- (a) an imminent risk of serious harm to a person or substantial damage to property exists; and
 - (b) the order is necessary for the purpose of dealing with that risk; and
 - (c) it is not practicable in the circumstances to make the application in writing.
- (2) For the purposes of this Schedule, it is necessary, because of urgent circumstances, to make an application under Part 4 of this Schedule for an international production order by telephone if, and only if:
- (a) the delay caused by making a written application may be prejudicial to security; and
 - (b) it is not practicable in the circumstances to make the application in writing.
- (3) For the purposes of this Schedule, it is necessary, because of urgent circumstances, for the Attorney-General to consent orally to the making of an application under Part 4 of this Schedule for an international production order if, and only if:
- (a) the delay caused by consenting in writing may be prejudicial to security; and
 - (b) it is not practicable in the circumstances to consent in writing.

18 Meaning of expressions in other provisions of this Act

In determining the meaning of an expression (other than “international production order”) used in a provision of this Act (other than this Schedule), an expression used in this Schedule is to be disregarded.

19 Extra-territorial application

This Schedule extends to acts, omissions, matters and things outside Australia.

20 Constitutional basis of this Schedule

This Schedule relies on the Commonwealth's legislative powers under paragraph 51(v) (communications) of the Constitution.

Part 2—International production orders relating to the enforcement of the criminal law

Division 1—Introduction

21 Simplified outline of this Part

- An international production order may be issued for purposes in connection with the investigation of an offence of a serious nature.
- There are 3 types of international production orders:
 - (a) international production orders relating to interception; and
 - (b) international production orders relating to stored communications; and
 - (c) international production orders relating to telecommunications data.
- An international production order is directed to a prescribed communications provider.
- An international production order may be issued in response to an application made by:
 - (a) in the case of an order relating to interception—an interception agency; or
 - (b) in the case of an order relating to stored communications—a criminal-law enforcement agency; or
 - (c) in the case of an order relating to telecommunications data—an enforcement agency.
- An application for an international production order must nominate a designated international agreement.

Note: An international production order comes into force when it is given to a prescribed communications provider under clause 111.

Schedule 1 International production orders

Part 2 International production orders relating to the enforcement of the criminal law

Division 2 International production orders relating to interception: enforcement of the criminal law

Clause 22

Division 2—International production orders relating to interception: enforcement of the criminal law

Subdivision A—Applications

22 Application for international production order—enforcement of the criminal law

- (1) An interception agency may apply to an eligible Judge or nominated AAT member for an international production order under clause 30 that:
 - (a) is in respect of:
 - (i) one or more individual transmission services; or
 - (ii) one or more individual message/call application services; and
 - (b) is directed to a prescribed communications provider.
- (2) The application must nominate a designated international agreement.
- (3) The application must be made on the interception agency's behalf by:
 - (a) in the case of the Australian Federal Police—a member of the Australian Federal Police; or
 - (b) in the case of the Australian Commission for Law Enforcement Integrity:
 - (i) the Integrity Commissioner; or
 - (ii) an Assistant Integrity Commissioner; or
 - (iii) a staff member of the Australian Commission for Law Enforcement Integrity who is authorised in writing by the Integrity Commissioner for the purposes of this paragraph; or
 - (c) in the case of the ACC:
 - (i) the Chief Executive Officer of the ACC or an examiner; or

- (ii) a member of a police force who is a member of the staff of the ACC; or
- (d) in the case of the Police Force of a State—an officer of that Police Force; or
- (e) in the case of the Crime Commission:
 - (i) a member of the Crime Commission; or
 - (ii) a member of the staff of the Crime Commission; or
- (f) in the case of the Independent Commission Against Corruption—an officer of that Commission; or
- (g) in the case of the IBAC—an IBAC officer; or
- (h) in the case of the Crime and Corruption Commission—a commission officer (within the meaning of the Crime and Corruption Act); or
- (i) in the case of the Law Enforcement Conduct Commission:
 - (i) the Chief Commissioner of the Commission; or
 - (ii) the Commissioner for Integrity of the Commission; or
 - (iii) an Assistant Commissioner of the Commission; or
 - (iv) a member of the staff of the Law Enforcement Conduct Commission; or
- (j) in the case of the Corruption and Crime Commission—an officer of the Corruption and Crime Commission; or
- (k) in the case of the Independent Commissioner Against Corruption:
 - (i) the Independent Commissioner Against Corruption; or
 - (ii) the Deputy Commissioner referred to in section 9 of the Independent Commissioner Against Corruption Act; or
 - (iii) a member of the staff of the Independent Commissioner Against Corruption.

23 Form of application

- (1) Subject to subclause (2), an application under clause 22 for an international production order must be in writing.

Schedule 1 International production orders

Part 2 International production orders relating to the enforcement of the criminal law

Division 2 International production orders relating to interception: enforcement of the criminal law

Clause 24

- (2) If the person making an application under clause 22 for an international production order on an interception agency's behalf:
- (a) is the chief officer of the agency or a person in relation to whom an authorisation by the chief officer is in force under subclause (3); and
 - (b) thinks it necessary, because of urgent circumstances, to make the application by telephone;
- the person may make the application by telephone.

Note: See also clause 17A (urgent circumstances) and clause 172 (action required).

- (3) The chief officer of an interception agency may authorise in writing, for the purposes of subclause (2), persons who, or classes of persons who, are entitled under clause 22 to make applications on the agency's behalf.

24 Contents of application

A written application under clause 22 by an interception agency for an international production order must set out:

- (a) the name of the agency; and
- (b) the name of the person making the application on the agency's behalf.

25 Affidavits to accompany written application

- (1) A written application under clause 22 by an interception agency for an international production order must be accompanied by an affidavit complying with this clause.
- (2) The affidavit must set out the facts and other grounds on which the application is based.
- (3) If the application is for an international production order in respect of one or more individual transmission services, the affidavit must set out the following information, so far as it can be derived from the interception agency's records:

- (a) the number of previous applications (if any) for international production orders that the agency has made under clause 22 in relation to those individual transmission services;
 - (b) the number of international production orders (if any) previously issued in response to such applications;
 - (c) particulars of the use made by the agency of intercepted communications made available to the agency under such orders.
- (4) If the application is for an international production order in respect of one or more individual message/call application services, the affidavit must set out the following information, so far as it can be derived from the interception agency's records:
- (a) the number of previous applications (if any) for international production orders that the agency has made under clause 22 in relation to those individual message/call application services;
 - (b) the number of international production orders (if any) previously issued in response to such applications;
 - (c) particulars of the use made by the agency of intercepted messages, voice calls or video calls made available to the agency under such orders.
- (5) Despite subclause (1), a written application may be accompanied by 2 or more affidavits that together set out each matter that, apart from this subclause, this clause would have required an affidavit accompanying the application to set out.

26 Information to be given on telephone application

The information given to an eligible Judge or nominated AAT member in connection with a telephone application under clause 22 to the eligible Judge or nominated AAT member:

- (a) must include particulars of the urgent circumstances because of which the person making the application on the interception agency's behalf thinks it necessary to make the application by telephone; and

Schedule 1 International production orders

Part 2 International production orders relating to the enforcement of the criminal law

Division 2 International production orders relating to interception: enforcement of the criminal law

Clause 27

- (b) must include each matter that, if the application had been made in writing, clause 24 or 25 would have required the application, or an affidavit accompanying it, to set out; and
- (c) must be given orally or in writing, as the eligible Judge or nominated AAT member directs.

27 Giving further information to eligible Judge or nominated AAT member

- (1) An eligible Judge or nominated AAT member may require further information to be given in connection with an application under clause 22 to the eligible Judge or nominated AAT member for an international production order.
- (2) The further information:
 - (a) must be given on oath if the application was made in writing; and
 - (b) must be given orally or otherwise, as the eligible Judge or nominated AAT member directs.

28 Application by interception agency of Victoria

Scope

- (1) This clause applies if an interception agency of Victoria applies, under clause 22, to an eligible Judge or nominated AAT member for an international production order under clause 30 that is in respect of:
 - (a) one or more individual transmission services; or
 - (b) one or more individual message/call application services.

PIM may make submissions

- (2) A Victorian PIM may, orally or in writing, make submissions to the eligible Judge or nominated AAT member about the following matters:
 - (a) in the case of an application for an international production order that is in respect of one or more individual transmission

services—the matters mentioned in subparagraphs 30(5)(a)(i) to (vi);

- (b) in the case of an application for an international production order that is in respect of one or more individual message/call application services—the matters mentioned in subparagraphs 30(5)(b)(i) to (vi).

PIM may question certain persons

- (3) The Victorian PIM may, for the purpose of making submissions under subclause (2), question:
 - (a) the person making the application for the international production order on the interception agency's behalf; or
 - (b) a person who, under clause 27, is required by the eligible Judge or nominated AAT member to give further information to the eligible Judge or nominated AAT member in connection with the application.

However, the Victorian PIM may only do so in the presence of the eligible Judge or nominated AAT member.

29 Application by interception agency of Queensland

Scope

- (1) This clause applies if an interception agency of Queensland applies, under clause 22, to an eligible Judge or nominated AAT member for an international production order under clause 30 that is in respect of:
 - (a) one or more individual transmission services; or
 - (b) one or more individual message/call application services.

PIM may make submissions

- (2) A Queensland PIM may, orally or in writing, make submissions to the eligible Judge or nominated AAT member about the following matters:

Schedule 1 International production orders

Part 2 International production orders relating to the enforcement of the criminal law

Division 2 International production orders relating to interception: enforcement of the criminal law

Clause 30

- (a) in the case of an application for an international production order that is in respect of one or more individual transmission services—the matters mentioned in subparagraphs 30(5)(a)(i) to (vi);
- (b) in the case of an application for an international production order that is in respect of one or more individual message/call application services—the matters mentioned in subparagraphs 30(5)(b)(i) to (vi).

PIM may question certain persons

- (3) The Queensland PIM may, for the purpose of making submissions under subclause (2), question:
 - (a) the person making the application for the international production order on the interception agency's behalf; or
 - (b) a person who, under clause 27, is required by the eligible Judge or nominated AAT member to give further information to the eligible Judge or nominated AAT member in connection with the application.

However, the Queensland PIM may only do so in the presence of the eligible Judge or nominated AAT member.

- (4) A Queensland PIM may, by writing, delegate to a Queensland deputy PIM the Queensland PIM's power under subclause (2) or (3), or both.
- (5) In exercising powers under the delegation, the Queensland deputy PIM must comply with any directions of the Queensland PIM.

Subdivision B—International production orders relating to interception

30 Issue of international production order—enforcement of the criminal law

Scope

- (1) This clause applies if an interception agency applies, under clause 22, to an eligible Judge or nominated AAT member for an international production order that:
 - (a) is in respect of:
 - (i) one or more individual transmission services; or
 - (ii) one or more individual message/call application services; and
 - (b) is directed to a prescribed communications provider.

Issue of international production order

- (2) If the eligible Judge or nominated AAT member is satisfied, on the basis of the information given to the eligible Judge or nominated AAT member under this Division in connection with the application, that:
 - (a) in the case of an application for an international production order that is in respect of one or more individual transmission services—there are reasonable grounds for suspecting that:
 - (i) the prescribed communications provider owns or operates a telecommunications network that is, or is likely to be, used to supply those individual transmission services; or
 - (ii) the prescribed communications provider supplies those individual transmission services; and
 - (b) in the case of an application for an international production order that is in respect of one or more individual message/call application services—there are reasonable grounds for suspecting that the prescribed communications provider

Schedule 1 International production orders

Part 2 International production orders relating to the enforcement of the criminal law

Division 2 International production orders relating to interception: enforcement of the criminal law

Clause 30

provides those individual message/call application services;
and

- (ba) the person who made the application on behalf of the agency reasonably suspects that the prescribed communications provider is based in, or operates in, a foreign country that is a party to the designated international agreement nominated in the application; and
- (c) Subdivision A has been complied with in relation to the application; and
- (d) in the case of a telephone application—because of urgent circumstances, it was necessary to make the application by telephone; and
- (e) in the case of an application for an international production order that is in respect of one or more individual transmission services—there are reasonable grounds for suspecting that a particular person is using, or is likely to use, those individual transmission services; and
- (f) in the case of an application for an international production order that is in respect of one or more individual message/call application services—there are reasonable grounds for suspecting that a particular person is using, or is likely to use, those individual message/call application services; and
- (g) in the case of an application for an international production order that is in respect of one or more individual transmission services—information that would be likely to be obtained by intercepting, under an order issued under this clause, communications that are being carried by those individual transmission services would be likely to assist in connection with the investigation by the interception agency of a serious category 2 offence, or serious category 2 offences, in which:
 - (i) the particular person is involved; or
 - (ii) another person is involved with whom the particular person is likely to communicate using those individual transmission services; and
- (h) in the case of an application for an international production order that is in respect of one or more individual message/call

application services—information that would be likely to be obtained by intercepting, under an order issued under this clause, messages sent or received, voice calls made or received, or video calls made or received, using those individual message/call application services would be likely to assist in connection with the investigation by the interception agency of a serious category 2 offence, or serious category 2 offences, in which:

- (i) the particular person is involved; or
- (ii) another person is involved with whom the particular person is likely to communicate using those individual message/call application services;

the eligible Judge or nominated AAT member may issue an order (to be known as an ***international production order***) directing the prescribed communications provider to:

- (i) in the case of an application for an international production order that is in respect of one or more individual transmission services:
 - (i) intercept communications carried by those individual transmission services during a specified period; and
 - (ii) make those intercepted communications available to the interception agency; and
 - (iii) disclose to the interception agency specified telecommunications data that relates to those intercepted communications; and
 - (iv) disclose to the interception agency specified telecommunications data that relates to those individual transmission services; or
- (j) in the case of an application for an international production order that is in respect of one or more individual message/call application services:
 - (i) intercept messages sent or received, voice calls made or received, or video calls made or received, using those individual message/call application services during a specified period; and

Schedule 1 International production orders

Part 2 International production orders relating to the enforcement of the criminal law

Division 2 International production orders relating to interception: enforcement of the criminal law

Clause 30

- (ii) make those intercepted messages, voice calls or video calls available to the interception agency; and
- (iii) disclose to the interception agency specified telecommunications data that relates to those intercepted messages, voice calls or video calls; and
- (iv) disclose to the interception agency specified telecommunications data that relates to those individual message/call application services.

Note: Subclauses (6) and (7) restrict the issuing of international production orders if subparagraph (2)(g)(ii) or (h)(ii) applies.

Period specified in international production order

- (3) A period specified in an international production order for the purposes of subparagraph (2)(i)(i) or (j)(i) must not begin before the time when the order is given to the prescribed communications provider.

Note: International production orders are given under clause 111.

- (4) The period specified in an international production order for the purposes of subparagraph (2)(i)(i) or (j)(i) must not be longer than:
 - (a) if subparagraph (2)(g)(ii) or (h)(ii) applies (as the case requires)—45 days; or
 - (b) otherwise—90 days.

Matters to which eligible Judge or nominated AAT member must have regard

- (5) In deciding whether to issue an international production order under subclause (2), the eligible Judge or nominated AAT member must have regard to the following matters:
 - (a) in the case of an application for an international production order that is in respect of one or more individual transmission services:
 - (i) how much the privacy of any person or persons would be likely to be interfered with by intercepting, under an international production order, communications that are

- being carried by those individual transmission services;
and
- (ii) the gravity of the conduct constituting the serious category 2 offence or serious category 2 offences being investigated; and
 - (iii) how much the information mentioned in paragraph (2)(g) would be likely to assist in connection with the investigation by the interception agency of the serious category 2 offence or serious category 2 offences; and
 - (iv) to what extent methods of investigating the serious category 2 offence or serious category 2 offences that do not involve so intercepting communications have been used by, or are available to, the interception agency; and
 - (v) how much the use of such methods would be likely to assist in connection with the investigation by the interception agency of the serious category 2 offence or serious category 2 offences; and
 - (vi) how much the use of such methods would be likely to prejudice the investigation by the interception agency of the serious category 2 offence or serious category 2 offences, whether because of delay or for any other reason; and
 - (vii) in relation to an application by an interception agency of Victoria—any submissions made by a Victorian PIM under clause 28 to the eligible Judge or nominated AAT member; and
 - (viii) in relation to an application by an interception agency of Queensland—any submissions made by a Queensland PIM under clause 29 to the eligible Judge or nominated AAT member; and
 - (ix) such other matters (if any) as the eligible Judge or nominated AAT member considers relevant;

Schedule 1 International production orders

Part 2 International production orders relating to the enforcement of the criminal law

Division 2 International production orders relating to interception: enforcement of the criminal law

Clause 30

- (b) in the case of an application for an international production order that is in respect of one or more individual message/call application services:
- (i) how much the privacy of any person or persons would be likely to be interfered with by intercepting, under an international production order, messages sent or received, voice calls made or received, or video calls made or received, using those individual message/call application services; and
 - (ii) the gravity of the conduct constituting the serious category 2 offence or serious category 2 offences being investigated; and
 - (iii) how much the information mentioned in paragraph (2)(h) would be likely to assist in connection with the investigation by the interception agency of the serious category 2 offence or serious category 2 offences; and
 - (iv) to what extent methods of investigating the serious category 2 offence or serious category 2 offences that do not involve so intercepting messages, voice calls or video calls have been used by, or are available to, the interception agency; and
 - (v) how much the use of such methods would be likely to assist in connection with the investigation by the interception agency of the serious category 2 offence or serious category 2 offences; and
 - (vi) how much the use of such methods would be likely to prejudice the investigation by the interception agency of the serious category 2 offence or serious category 2 offences, whether because of delay or for any other reason; and
 - (vii) in relation to an application by an interception agency of Victoria—any submissions made by a Victorian PIM under clause 28 to the eligible Judge or nominated AAT member; and

- (viii) in relation to an application by an interception agency of Queensland—any submissions made by a Queensland PIM under clause 29 to the eligible Judge or nominated AAT member; and
- (ix) such other matters (if any) as the eligible Judge or nominated AAT member considers relevant.

Restriction on issuing order

- (6) The eligible Judge or nominated AAT member must not issue an international production order under subclause (2) in a case where subparagraph (2)(g)(ii) applies unless the eligible Judge or nominated AAT member is satisfied that:
 - (a) the interception agency has exhausted all other practicable methods of identifying the individual transmission services used, or likely to be used, by the person involved in the serious category 2 offence or serious category 2 offences mentioned in paragraph (2)(g); or
 - (b) interception of communications carried by individual transmission services used or likely to be used by that person would not otherwise be possible.
- (7) The eligible Judge or nominated AAT member must not issue an international production order under subclause (2) in a case where subparagraph (2)(h)(ii) applies unless the eligible Judge or nominated AAT member is satisfied that:
 - (a) the interception agency has exhausted all other practicable methods of identifying the individual message/call application services used, or likely to be used, by the person involved in the serious category 2 offence or serious category 2 offences mentioned in paragraph (2)(h); or
 - (b) interception of messages sent or received, voice calls made or received, or video calls made or received, using individual message/call application services used or likely to be used by that person would not otherwise be possible.

Schedule 1 International production orders

Part 2 International production orders relating to the enforcement of the criminal law

Division 2 International production orders relating to interception: enforcement of the criminal law

Clause 31

31 Content of international production order

Scope

- (1) This clause applies to an international production order issued under clause 30 in response to an application made by an interception agency.

Content

- (2) The order must be signed by the eligible Judge or nominated AAT member who issued it.
- (3) The order must set out the following:
- (a) the date on which the order was issued;
 - (b) the name of the interception agency;
 - (c) the name of the prescribed communications provider to whom the order is directed;
 - (d) the name of the designated international agreement nominated in the application for the order;
 - (e) the applicable telecommunications identifiers:
 - (i) in the case of an order that is in respect of one or more individual transmission services—to which those individual transmission services relate; or
 - (ii) in the case of an order that is in respect of one or more individual message/call application services—to which those individual message/call application services relate;
 - (f) short particulars of each serious category 2 offence in relation to which the eligible Judge or nominated AAT member issuing the order was satisfied, on the application for the order, as mentioned in paragraph 30(2)(g) or (h) of this Schedule (as the case requires).
- (4) If the order directs a prescribed communications provider to intercept communications, the order may require the provider to:
- (a) intercept those communications in a specified way; and

- (b) make those intercepted communications available to the interception agency in a specified way.
- (5) A requirement under subclause (4) may:
 - (a) require that intercepted communications be made available to the interception agency directly; or
 - (b) require that intercepted communications be made available to the interception agency indirectly via the Australian Designated Authority.
- (6) If the order directs a prescribed communications provider to intercept messages, voice calls or video calls, the order may require the provider to:
 - (a) intercept those messages, voice calls or video calls in a specified way; and
 - (b) make those intercepted messages, voice calls or video calls available to the interception agency in a specified way.
- (7) A requirement under subclause (6) may:
 - (a) require that intercepted messages, voice calls or video calls be made available to the interception agency directly; or
 - (b) require that intercepted messages, voice calls or video calls be made available to the interception agency indirectly via the Australian Designated Authority.
- (8) If the order directs a prescribed communications provider to disclose telecommunications data to the interception agency, the order may require the provider to disclose that data to the agency in a specified way.
- (9) A requirement under subclause (8) may:
 - (a) require that the telecommunications data be disclosed to the interception agency directly; or
 - (b) require that the telecommunications data be disclosed to the interception agency indirectly via the Australian Designated Authority.

Schedule 1 International production orders

Part 2 International production orders relating to the enforcement of the criminal law

Division 2 International production orders relating to interception: enforcement of the criminal law

Clause 32

- (10) For the purposes of this clause, a specified way may deal with matters of timing.

Example: A requirement under subclause (4) may require that an intercepted communication be made available to the interception agency within 30 minutes after the communication was completed.

32 Issue of further international production order

- (1) If:

- (a) an international production order (the *original order*) was issued under clause 30; and
- (b) the original order was in respect of one or more individual transmission services; and
- (c) the original order was directed to a prescribed communications provider;

this Schedule does not prevent the issue of a further international production order under clause 30 that is:

- (d) in respect of any or all of those services; and
- (e) directed to the provider;

so long as the period specified in the further order for the purposes of subparagraph 30(2)(i)(i) of this Schedule begins after the end of the period specified in the original order for the purposes of that subparagraph.

- (2) If:

- (a) an international production order (the *original order*) was issued under clause 30; and
- (b) the original order was in respect of one or more individual message/call application services; and
- (c) the original order was directed to a prescribed communications provider;

this Schedule does not prevent the issue of a further international production order under clause 30 that is:

- (d) in respect of any or all of those services; and
- (e) directed to the provider;

so long as the period specified in the further order for the purposes of subparagraph 30(2)(j)(i) of this Schedule begins after the end of the period specified in the original order for the purposes of that subparagraph.

Schedule 1 International production orders

Part 2 International production orders relating to the enforcement of the criminal law

Division 3 International production orders relating to stored communications:
enforcement of the criminal law

Clause 33

**Division 3—International production orders relating to
stored communications: enforcement of the
criminal law**

Subdivision A—Applications

**33 Application for international production order—enforcement of
the criminal law**

- (1) A criminal law-enforcement agency may apply to an issuing authority for an international production order under clause 39 that:
 - (a) is in respect of a particular person; and
 - (b) is directed to a prescribed communications provider.
- (2) The application must nominate a designated international agreement.
- (3) The application must be made on the criminal law-enforcement agency's behalf by:
 - (a) if the agency is referred to in subclause 22(3)—a person referred to in that subclause in relation to the agency; or
 - (b) otherwise:
 - (i) the chief officer of the agency; or
 - (ii) an officer of the agency (by whatever name called) who holds, or is acting in, an office or position in the agency nominated under subclause (4).
- (4) The chief officer of the criminal law-enforcement agency may, in writing, nominate for the purposes of subparagraph (3)(b)(ii) an office or position in the agency that is involved in the management of the agency.
- (5) A nomination under subclause (4) is not a legislative instrument.

34 Form of application

- (1) An application under clause 33 must be in writing.
- (2) However, a person making the application on the criminal law-enforcement agency's behalf may make the application by telephone if the person:
 - (a) is the chief officer of the agency or a person in relation to whom an authorisation by the chief officer is in force under subclause (3); and
 - (b) thinks it necessary, because of urgent circumstances, to make the application by telephone.

Note: See also clause 17A (urgent circumstances) and clause 172 (action required).

- (3) The chief officer of a criminal law-enforcement agency may, in writing, authorise persons (including classes of persons) for the purposes of subclause (2). However, each person must be entitled under clause 33 to make applications on the agency's behalf.

35 Contents of written application

An application under clause 33 must, if it is in writing, set out:

- (a) the name of the criminal law-enforcement agency; and
- (b) the name of the person making the application on the agency's behalf.

36 Affidavits to accompany written application

- (1) An application under clause 33 must, if it is in writing, be accompanied by an affidavit complying with this clause.
- (2) The affidavit must set out the facts and other grounds on which the application is based.
- (3) Despite subclause (1), a written application may be accompanied by 2 or more affidavits that together set out each matter that, apart from this subclause, this clause would have required an affidavit accompanying the application to set out.

Schedule 1 International production orders

Part 2 International production orders relating to the enforcement of the criminal law

Division 3 International production orders relating to stored communications:
enforcement of the criminal law

Clause 37

37 Information to be given on telephone application

The information given to an issuing authority in connection with a telephone application under clause 33 to the issuing authority:

- (a) must include particulars of the urgent circumstances because of which the person making the application on the criminal law-enforcement agency's behalf thinks it necessary to make the application by telephone; and
- (b) must include each matter that, if the application had been made in writing, clause 35 or 36 would have required the application, or an affidavit accompanying it, to set out; and
- (c) must be given orally or in writing, as the issuing authority directs.

38 Giving further information to issuing authority

- (1) An issuing authority may require further information to be given in connection with an application under clause 33 to the issuing authority for an international production order.
- (2) The further information:
 - (a) must be given on oath if the application was made in writing; and
 - (b) must be given orally or otherwise, as the issuing authority directs.

Subdivision B—International production orders relating to stored communications

39 Issue of international production order—enforcement of the criminal law

Scope

- (1) This clause applies if a criminal law-enforcement agency applies, under clause 33, to an issuing authority for an international production order that:

- (a) is in respect of a particular person (the *relevant person*); and
- (b) is directed to a prescribed communications provider.

Issue of international production order

- (2) If the issuing authority is satisfied, on the basis of the information given to the issuing authority under this Division in connection with the application, that:
 - (a) there are reasonable grounds for suspecting that the prescribed communications provider holds any of the following stored communications:
 - (i) stored communications that consist of communications that the relevant person has made using a telecommunications network owned or operated by the prescribed communications provider;
 - (ii) stored communications that consist of communications that another person has made using a telecommunications network owned or operated by the prescribed communications provider, and for which the relevant person is the intended recipient;
 - (iii) stored communications that consist of communications that the relevant person has made using a transmission service supplied by the prescribed communications provider;
 - (iv) stored communications that consist of communications that another person has made using a transmission service supplied by the prescribed communications provider, and for which the relevant person is the intended recipient;
 - (v) stored communications that consist of messages that the relevant person has sent or received using a message/call application service provided by the prescribed communications provider;
 - (vi) stored communications that consist of recordings of voice calls that the relevant person has made or received using a message/call application service provided by the prescribed communications provider;

Schedule 1 International production orders

Part 2 International production orders relating to the enforcement of the criminal law

Division 3 International production orders relating to stored communications:
enforcement of the criminal law

Clause 39

- (vii) stored communications that consist of recordings of video calls that the relevant person has made or received using a message/call application service provided by the prescribed communications provider;
 - (viii) stored communications that consist of material that the relevant person has uploaded for storage or back-up by a storage/back-up service provided by the prescribed communications provider;
 - (ix) stored communications that consist of material that the relevant person has posted to a general electronic content service provided by the prescribed communications provider; and
- (aa) the person who made the application on behalf of the agency reasonably suspects that the prescribed communications provider is based in, or operates in, a foreign country that is a party to the designated international agreement nominated in the application; and
 - (b) Subdivision A has been complied with in relation to the application; and
 - (c) in the case of a telephone application—because of urgent circumstances, it was necessary to make the application by telephone; and
 - (d) information that would be likely to be obtained by making a copy, under an order issued under this clause, of the stored communications would be likely to assist in connection with the investigation by the criminal law-enforcement agency of a serious category 1 offence, or serious category 1 offences, in which the relevant person is involved;
- the issuing authority may issue an order (to be known as an ***international production order***) directing the prescribed communications provider to:
- (e) make a copy of any such stored communications; and
 - (f) make the copy available to the criminal law-enforcement agency; and

- (g) if the stored communications consist of communications carried by an individual transmission service—disclose to the agency:
 - (i) specified telecommunications data that relates to those communications; and
 - (ii) specified telecommunications data that relates to the individual transmission service; and
 - (h) if the stored communications consist of messages sent or received using an individual message/call application service—disclose to the agency:
 - (i) specified telecommunications data that relates to those messages; and
 - (ii) specified telecommunications data that relates to the individual message/call application service; and
 - (i) if the stored communications consist of recordings of voice calls made or received using an individual message/call application service—disclose to the agency:
 - (i) specified telecommunications data that relates to those voice calls; and
 - (ii) specified telecommunications data that relates to the individual message/call application service; and
 - (j) if the stored communications consist of recordings of video calls made or received using an individual message/call application service—disclose to the agency:
 - (i) specified telecommunications data that relates to those video calls; and
 - (ii) specified telecommunications data that relates to the individual message/call application service; and
 - (k) if the stored communications consist of material that has been uploaded by an end-user for storage or back-up by a storage/back-up service—disclose to the agency:
 - (i) specified telecommunications data that relates to that material; and
 - (ii) specified telecommunications data that relates to the end-user’s account with the storage/back-up service; and
-

Schedule 1 International production orders

Part 2 International production orders relating to the enforcement of the criminal law

Division 3 International production orders relating to stored communications:
enforcement of the criminal law

Clause 39

- (l) if the stored communications consist of material posted to a general electronic content service by an end-user—disclose to the agency:
 - (i) specified telecommunications data that relates to that material; and
 - (ii) specified telecommunications data that relates to the end-user’s account with the general electronic content service.

Matters to which issuing authority must have regard

- (3) In deciding whether to issue an international production order under subclause (2), the issuing authority must have regard to the following matters:
 - (a) how much the privacy of any person or persons would be likely to be interfered with by the criminal law-enforcement agency obtaining, under an international production order, a copy of the stored communications;
 - (b) the gravity of the conduct constituting the serious category 1 offence or serious category 1 offences being investigated;
 - (c) how much the information mentioned in paragraph (2)(d) would be likely to assist in connection with the investigation by the criminal law-enforcement agency of the serious category 1 offence or serious category 1 offences;
 - (d) to what extent methods of investigating the serious category 1 offence or serious category 1 offences that do not involve so obtaining a copy of the stored communications have been used by, or are available to, the criminal law-enforcement agency;
 - (e) how much the use of such methods would be likely to assist in connection with the investigation by the criminal law-enforcement agency of the serious category 1 offence or serious category 1 offences;
 - (f) how much the use of such methods would be likely to prejudice the investigation by the criminal law-enforcement agency of the serious category 1 offence or serious category 1 offences, whether because of delay or for any other reason;

- (g) such other matters (if any) as the issuing authority considers relevant.

40 Content of international production order

Scope

- (1) This clause applies to an international production order issued under clause 39 in response to an application made by a criminal law-enforcement agency.

Content

- (2) The order must be signed by the issuing authority who issued it.
- (3) The order must set out the following:
- (a) the date on which the order was issued;
 - (b) the name of the criminal law-enforcement agency;
 - (c) the name of the prescribed communications provider to whom the order is directed;
 - (d) the name of the designated international agreement nominated in the application for the order;
 - (e) short particulars of each serious category 1 offence in relation to which the issuing authority issuing the order was satisfied, on the application for the order, as mentioned in paragraph 39(2)(d) of this Schedule.
- (4) If the order directs a prescribed communications provider to make a copy of stored communications available to the criminal law-enforcement agency, the order may require the provider to make that copy available to the agency in a specified way.
- (5) A requirement under subclause (4) may:
- (a) require that a copy of stored communications be made available to the criminal law-enforcement agency directly; or
 - (b) require that a copy of stored communications be made available to the criminal law-enforcement agency indirectly via the Australian Designated Authority.

Schedule 1 International production orders

Part 2 International production orders relating to the enforcement of the criminal law

Division 3 International production orders relating to stored communications:
enforcement of the criminal law

Clause 41

- (6) If the order directs a prescribed communications provider to disclose telecommunications data to the criminal law-enforcement agency, the order may require the provider to disclose that data to the agency in a specified way.
- (7) A requirement under subclause (6) may:
 - (a) require that the telecommunications data be disclosed to the criminal law-enforcement agency directly; or
 - (b) require that the telecommunications data be disclosed to the criminal law-enforcement agency indirectly via the Australian Designated Authority.
- (8) For the purposes of this clause, a specified way may deal with matters of timing.

41 Issue of further international production order

If:

- (a) an international production order (the *original order*) was issued under clause 39; and
- (b) the original order was in respect of a particular person; and
- (c) the original order was directed to a prescribed communications provider;

this Schedule does not prevent the issue of a further international production order under clause 39 that:

- (d) is in respect of the person; and
- (e) is directed to the provider.

Division 4—International production orders relating to telecommunications data: enforcement of the criminal law

Subdivision A—Applications

42 Application for international production order—enforcement of the criminal law

- (1) An enforcement agency may apply to an issuing authority for an international production order under clause 48 that is directed to a prescribed communications provider.
- (2) The application must nominate a designated international agreement.
- (3) The application must be made on the enforcement agency's behalf by an authorised officer of the agency.

43 Form of application

- (1) An application under clause 42 must be in writing.
- (2) However, a person making the application on the enforcement agency's behalf may make the application by telephone if the person:
 - (a) is the chief officer of the agency or a person in relation to whom an authorisation by the chief officer is in force under subclause (3); and
 - (b) thinks it necessary, because of urgent circumstances, to make the application by telephone.

Note: See also clause 17A (urgent circumstances) and clause 172 (action required).

- (3) The chief officer of an enforcement agency may, in writing, authorise persons (including classes of persons) for the purposes of

Schedule 1 International production orders

Part 2 International production orders relating to the enforcement of the criminal law

Division 4 International production orders relating to telecommunications data:
enforcement of the criminal law

Clause 44

subclause (2). However, each person must be entitled under clause 42 to make applications on the agency's behalf.

44 Contents of written application

An application under clause 42 must, if it is in writing, set out:

- (a) the name of the enforcement agency; and
- (b) the name of the person making the application on the agency's behalf.

45 Affidavits to accompany written application

- (1) An application under clause 42 must, if it is in writing, be accompanied by an affidavit complying with this clause.
- (2) The affidavit must set out the facts and other grounds on which the application is based.
- (3) Despite subclause (1), a written application may be accompanied by 2 or more affidavits that together set out each matter that, apart from this subclause, this clause would have required an affidavit accompanying the application to set out.

46 Information to be given on telephone application

The information given to an issuing authority in connection with a telephone application under clause 42 to the issuing authority:

- (a) must include particulars of the urgent circumstances because of which the person making the application on the enforcement agency's behalf thinks it necessary to make the application by telephone; and
- (b) must include each matter that, if the application had been made in writing, clause 44 or 45 would have required the application, or an affidavit accompanying it, to set out; and
- (c) must be given orally or in writing, as the issuing authority directs.

47 Giving further information to issuing authority

- (1) An issuing authority may require further information to be given in connection with an application under clause 42 to the issuing authority for an international production order.
- (2) The further information:
 - (a) must be given on oath if the application was made in writing; and
 - (b) must be given orally or otherwise, as the issuing authority directs.

Subdivision B—International production orders relating to telecommunications data

48 Issue of international production order—enforcement of the criminal law

Scope

- (1) This clause applies if an enforcement agency applies, under clause 42, to an issuing authority for an international production order that is directed to a prescribed communications provider.

Issue of international production order

- (2) If the issuing authority is satisfied, on the basis of the information given to the issuing authority under this Division in connection with the application, that:
 - (a) there are reasonable grounds for suspecting that the prescribed communications provider holds, or is likely to commence to hold, any of the following telecommunications data:
 - (i) telecommunications data that relates to communications carried by an individual transmission service supplied using a telecommunications network owned or operated by the prescribed communications provider;

Schedule 1 International production orders

Part 2 International production orders relating to the enforcement of the criminal law

Division 4 International production orders relating to telecommunications data:
enforcement of the criminal law

Clause 48

- (ii) telecommunications data that relates to an individual transmission service supplied using a telecommunications network owned or operated by the prescribed communications provider;
- (iii) telecommunications data that relates to communications carried by an individual transmission service supplied by the prescribed communications provider;
- (iv) telecommunications data that relates to an individual transmission service supplied by the prescribed communications provider;
- (v) telecommunications data that relates to messages sent or received using an individual message/call application service provided by the prescribed communications provider;
- (vi) telecommunications data that relates to voice calls made or received using an individual message/call application service provided by the prescribed communications provider;
- (vii) telecommunications data that relates to video calls made or received using an individual message/call application service provided by the prescribed communications provider;
- (viii) telecommunications data that relates to an individual message/call application service provided by the prescribed communications provider;
- (ix) telecommunications data that relates to material that has been uploaded by an end-user for storage or back-up by a storage/back-up service provided by the prescribed communications provider;
- (x) telecommunications data that relates to material that has been posted on a general electronic content service provided by the prescribed communications provider;
and
- (aa) the person who made the application on behalf of the agency reasonably suspects that the prescribed communications provider is based in, or operates in, a foreign country that is a

party to the designated international agreement nominated in the application; and

- (b) Subdivision A has been complied with in relation to the application; and
- (c) in the case of a telephone application—because of urgent circumstances, it was necessary to make the application by telephone; and
- (d) disclosing the telecommunications data to the enforcement agency, under an order issued under this clause, would be likely to assist in connection with the investigation by the enforcement agency of a serious category 1 offence, or serious category 1 offences;

the issuing authority may issue an order (to be known as an ***international production order***) directing the prescribed communications provider to do either or both of the following:

- (e) so far as the telecommunications data is held by the prescribed communications provider when the international production order comes into force—disclose any such telecommunications data to the agency;
- (f) so far as the telecommunications data commences to be held by the prescribed communications provider during a specified period—disclose any such telecommunications data to the agency.

Period specified in international production order

- (3) A period specified in an international production order for the purposes of paragraph (2)(f) must not begin before the time when the order is given to the prescribed communications provider.

Note: International production orders are given under clause 111.

- (4) A period specified in an international production order for the purposes of paragraph (2)(f) must not be longer than 90 days.

Schedule 1 International production orders

Part 2 International production orders relating to the enforcement of the criminal law

Division 4 International production orders relating to telecommunications data:
enforcement of the criminal law

Clause 49

Matters to which issuing authority must have regard

- (5) In deciding whether to issue an international production order under subclause (2), the issuing authority must have regard to the following matters:
- (a) how much the privacy of any person or persons would be likely to be interfered with by disclosing, under an international production order, the telecommunications data;
 - (b) the gravity of the conduct constituting the serious category 1 offence or serious category 1 offences being investigated;
 - (c) how much the telecommunications data would be likely to assist in connection with the investigation by the enforcement agency of the serious category 1 offence or serious category 1 offences;
 - (d) to what extent methods of investigating the serious category 1 offence or serious category 1 offences that do not involve so disclosing the telecommunications data have been used by, or are available to, the enforcement agency;
 - (e) how much the use of such methods would be likely to assist in connection with the investigation by the enforcement agency of the serious category 1 offence or serious category 1 offences;
 - (f) how much the use of such methods would be likely to prejudice the investigation by the enforcement agency of the serious category 1 offence or serious category 1 offences, whether because of delay or for any other reason;
 - (g) such other matters (if any) as the issuing authority considers relevant.

49 Content of international production order

Scope

- (1) This clause applies to an international production order issued under clause 48 in response to an application made by an enforcement agency.

Content

- (2) The order must be signed by the issuing authority who issued it.
- (3) The order must set out the following:
 - (a) the date on which the order was issued;
 - (b) the name of the enforcement agency;
 - (c) the name of the prescribed communications provider to whom the order is directed;
 - (d) the name of the designated international agreement nominated in the application for the order;
 - (e) short particulars of each serious category 1 offence in relation to which the issuing authority issuing the order was satisfied, on the application for the order, as mentioned in paragraph 48(2)(d) of this Schedule.
- (4) If the order directs a prescribed communications provider to disclose telecommunications data to the enforcement agency, the order may require the provider to disclose that data to the agency in a specified way.
- (5) A requirement under subclause (4) may:
 - (a) require that the telecommunications data be disclosed to the enforcement agency directly; or
 - (b) require that the telecommunications data be disclosed to the enforcement agency indirectly via the Australian Designated Authority.
- (6) For the purposes of this clause, a specified way may deal with matters of timing.

Example: If a requirement under subclause (4) relates to telecommunications data that commences to be held by a prescribed communications provider during a specified period, the requirement may require that the telecommunications data be disclosed to the enforcement agency within 30 minutes after the telecommunications data commences to be held.

Schedule 1 International production orders

Part 2 International production orders relating to the enforcement of the criminal law

Division 4 International production orders relating to telecommunications data:
enforcement of the criminal law

Clause 50

50 Issue of further international production order

If:

- (a) an international production order (the *original order*) was issued under clause 48; and
- (b) the original order was directed to a prescribed communications provider; and
- (c) the original order relates to the investigation by an enforcement agency of a serious category 1 offence, or serious category 1 offences;

this Schedule does not prevent the issue of a further international production order under clause 48 that:

- (d) is directed to the provider; and
- (e) relates to the investigation by the enforcement agency of that offence or those offences.

Part 3—International production orders relating to Part 5.3 supervisory orders

Division 1—Introduction

51 Simplified outline of this Part

- If a Part 5.3 supervisory order is in force in relation to a person, an international production order may be issued for purposes in connection with the monitoring of the person, so as to achieve a Part 5.3 object.
- There are 3 types of international production orders:
 - (a) international production orders relating to interception; and
 - (b) international production orders relating to stored communications; and
 - (c) international production orders relating to telecommunications data.
- An international production order is directed to a prescribed communications provider.
- An international production order may be issued in response to an application made by a Part 5.3 IPO agency.
- An application for an international production order must nominate a designated international agreement.
- If an international production order is issued in relation to an application made by a Part 5.3 IPO agency, the agency must notify the international production order to the Ombudsman.

Note: An international production order comes into force when it is given to a prescribed communications provider under clause 111.

Schedule 1 International production orders

Part 3 International production orders relating to Part 5.3 supervisory orders

Division 2 International production orders relating to interception: Part 5.3 supervisory orders

Clause 52

Division 2—International production orders relating to interception: Part 5.3 supervisory orders

Subdivision A—Applications

52 Application for international production order—Part 5.3 supervisory order

- (1) A Part 5.3 IPO agency may apply to an eligible Judge or nominated AAT member for an international production order under clause 60 that:
 - (a) is in respect of:
 - (i) one or more individual transmission services; or
 - (ii) one or more individual message/call application services; and
 - (b) is directed to a prescribed communications provider.
- (2) The application must nominate a designated international agreement.
- (3) The application must be made on the Part 5.3 IPO agency's behalf by:
 - (a) if the agency is referred to in subclause 22(3)—a person referred to in that subclause in relation to the agency; or
 - (b) otherwise:
 - (i) the chief officer of the agency; or
 - (ii) an officer of the agency (by whatever name called) who holds, or is acting in, an office or position in the agency nominated under subclause (4).
- (4) The chief officer of the Part 5.3 IPO agency may, in writing, nominate for the purposes of subparagraph (3)(b)(ii) an office or position in the agency that is involved in the management of the agency.

53 Form of application

- (1) Subject to subclause (2), an application under clause 52 for an international production order must be in writing.
- (2) If the person making an application under clause 52 for an international production order on a Part 5.3 IPO agency's behalf:
 - (a) is the chief officer of the agency or a person in relation to whom an authorisation by the chief officer is in force under subclause (3); and
 - (b) thinks it necessary, because of urgent circumstances, to make the application by telephone;the person may make the application by telephone.

Note: See also clause 17A (urgent circumstances) and clause 172 (action required).

- (3) The chief officer of a Part 5.3 IPO agency may authorise in writing, for the purposes of subclause (2), persons who, or classes of persons who, are entitled under clause 52 to make applications on the agency's behalf.

54 Contents of application

A written application under clause 52 by a Part 5.3 IPO agency for an international production order must set out:

- (a) the name of the agency; and
- (b) the name of the person making the application on the agency's behalf.

55 Affidavits to accompany written application

- (1) A written application under clause 52 by a Part 5.3 IPO agency for an international production order must be accompanied by an affidavit complying with this clause.
- (2) The affidavit must set out the facts and other grounds on which the application is based.

Schedule 1 International production orders

Part 3 International production orders relating to Part 5.3 supervisory orders

Division 2 International production orders relating to interception: Part 5.3 supervisory orders

Clause 56

- (3) If the application is for an international production order in respect of one or more individual transmission services, the affidavit must set out the following information, so far as it can be derived from the Part 5.3 IPO agency's records:
 - (a) the number of previous applications (if any) for international production orders that the agency has made under clause 52 in relation to those individual transmission services;
 - (b) the number of international production orders (if any) previously issued in response to such applications;
 - (c) particulars of the use made by the agency of intercepted communications made available to the agency under such orders.
- (4) If the application is for an international production order in respect of one or more individual message/call application services, the affidavit must set out the following information, so far as it can be derived from the Part 5.3 IPO agency's records:
 - (a) the number of previous applications (if any) for international production orders that the agency has made under clause 52 in relation to those individual message/call application services;
 - (b) the number of international production orders (if any) previously issued in response to such applications;
 - (c) particulars of the use made by the agency of intercepted messages, voice calls or video calls made available to the agency under such orders.
- (5) Despite subclause (1), a written application may be accompanied by 2 or more affidavits that together set out each matter that, apart from this subclause, this clause would have required an affidavit accompanying the application to set out.

56 Information to be given on telephone application

The information given to an eligible Judge or nominated AAT member in connection with a telephone application under clause 52 to the eligible Judge or nominated AAT member:

- (a) must include particulars of the urgent circumstances because of which the person making the application on the Part 5.3 IPO agency's behalf thinks it necessary to make the application by telephone; and
- (b) must include each matter that, if the application had been made in writing, clause 54 or 55 would have required the application, or an affidavit accompanying it, to set out; and
- (c) must be given orally or in writing, as the eligible Judge or nominated AAT member directs.

57 Giving further information to eligible Judge or nominated AAT member

- (1) An eligible Judge or nominated AAT member may require further information to be given in connection with an application under clause 52 to the eligible Judge or nominated AAT member for an international production order.
- (2) The further information:
 - (a) must be given on oath if the application was made in writing; and
 - (b) must be given orally or otherwise, as the eligible Judge or nominated AAT member directs.

58 Application by Part 5.3 IPO agency of Victoria

Scope

- (1) This clause applies if a Part 5.3 IPO agency of Victoria applies, under clause 52, to an eligible Judge or nominated AAT member for an international production order under clause 60 that is in respect of:
 - (a) one or more individual transmission services; or
 - (b) one or more individual message/call application services.

Schedule 1 International production orders

Part 3 International production orders relating to Part 5.3 supervisory orders

Division 2 International production orders relating to interception: Part 5.3 supervisory orders

Clause 59

PIM may make submissions

- (2) A Victorian PIM may, orally or in writing, make submissions to the eligible Judge or nominated AAT member about the following matters:
- (a) in the case of an application for an international production order that is in respect of one or more individual transmission services—the matters mentioned in paragraphs 60(5)(a) to (g);
 - (b) in the case of an application for an international production order that is in respect of one or more individual message/call application services—the matters mentioned in paragraphs 60(6)(a) to (g).

PIM may question certain persons

- (3) The Victorian PIM may, for the purpose of making submissions under subclause (2), question:
- (a) the person making the application for the international production order on the Part 5.3 IPO agency's behalf; or
 - (b) a person who, under clause 57, is required by the eligible Judge or nominated AAT member to give further information to the eligible Judge or nominated AAT member in connection with the application.

However, the Victorian PIM may only do so in the presence of the eligible Judge or nominated AAT member.

59 Application by Part 5.3 IPO agency of Queensland

Scope

- (1) This clause applies if a Part 5.3 IPO agency of Queensland applies, under clause 52, to an eligible Judge or nominated AAT member for an international production order under clause 60 that is in respect of:
- (a) one or more individual transmission services; or
 - (b) one or more individual message/call application services.

PIM may make submissions

- (2) A Queensland PIM may, orally or in writing, make submissions to the eligible Judge or nominated AAT member about the following matters:
- (a) in the case of an application for an international production order that is in respect of one or more individual transmission services—the matters mentioned in paragraphs 60(5)(a) to (g);
 - (b) in the case of an application for an international production order that is in respect of one or more individual message/call application services—the matters mentioned in paragraphs 60(6)(a) to (g).

PIM may question certain persons

- (3) The Queensland PIM may, for the purpose of making submissions under subclause (2), question:
- (a) the person making the application for the international production order on the Part 5.3 IPO agency's behalf; or
 - (b) a person who, under clause 57, is required by the eligible Judge or nominated AAT member to give further information to the eligible Judge or nominated AAT member in connection with the application.

However, the Queensland PIM may only do so in the presence of the eligible Judge or nominated AAT member.

- (4) A Queensland PIM may, by writing, delegate to a Queensland deputy PIM the Queensland PIM's power under subclause (2) or (3), or both.
- (5) In exercising powers under the delegation, the Queensland deputy PIM must comply with any directions of the Queensland PIM.

Schedule 1 International production orders

Part 3 International production orders relating to Part 5.3 supervisory orders

Division 2 International production orders relating to interception: Part 5.3 supervisory orders

Clause 60

Subdivision B—International production orders relating to interception

60 Issue of international production order—Part 5.3 supervisory order

Scope

- (1) This clause applies if a Part 5.3 IPO agency applies, under clause 52, to an eligible Judge or nominated AAT member for an international production order that:
 - (a) is in respect of:
 - (i) one or more individual transmission services; or
 - (ii) one or more individual message/call application services; and
 - (b) is directed to a prescribed communications provider.

Issue of international production order

- (2) If the eligible Judge or nominated AAT member is satisfied, on the basis of the information given to the eligible Judge or nominated AAT member under this Division in connection with the application, that:
 - (a) in the case of an application for an international production order that is in respect of one or more individual transmission services—there are reasonable grounds for suspecting that:
 - (i) the prescribed communications provider owns or operates a telecommunications network that is, or is likely to be, used to supply those individual transmission services; or
 - (ii) the prescribed communications provider supplies those individual transmission services; and
 - (b) in the case of an application for an international production order that is in respect of one or more individual message/call application services—there are reasonable grounds for suspecting that the prescribed communications provider

provides those individual message/call application services;
and

- (ba) the person who made the application on behalf of the agency reasonably suspects that the prescribed communications provider is based in, or operates in, a foreign country that is a party to the designated international agreement nominated in the application; and
- (c) Subdivision A has been complied with in relation to the application; and
- (d) in the case of a telephone application—because of urgent circumstances, it was necessary to make the application by telephone; and
- (e) in the case of an application for an international production order that is in respect of one or more individual transmission services—there are reasonable grounds for suspecting that a particular person is using, or is likely to use, those individual transmission services; and
- (f) in the case of an application for an international production order that is in respect of one or more individual message/call application services—there are reasonable grounds for suspecting that a particular person is using, or is likely to use, those individual message/call application services; and
- (g) in the case of an application for an international production order that is in respect of one or more individual transmission services:
 - (i) a Part 5.3 supervisory order is in force in relation to the particular person; or
 - (ii) a Part 5.3 supervisory order is in force in relation to another person, and the particular person is likely to communicate with the other person using those individual transmission services; and
- (h) in the case of an application for an international production order that is in respect of one or more individual message/call application services:
 - (i) a Part 5.3 supervisory order is in force in relation to the particular person; or

Schedule 1 International production orders

Part 3 International production orders relating to Part 5.3 supervisory orders

Division 2 International production orders relating to interception: Part 5.3 supervisory orders

Clause 60

- (ii) a Part 5.3 supervisory order is in force in relation to another person, and the particular person is likely to communicate with the other person using those individual message/call application services; and
- (i) in the case of an application for an international production order that is in respect of one or more individual transmission services—information that would be likely to be obtained by intercepting, under an order issued under this clause, communications that are being carried by those individual transmission services would be likely to substantially assist in connection with:
 - (i) achieving a Part 5.3 object; or
 - (ii) determining whether the Part 5.3 supervisory order, or any succeeding Part 5.3 supervisory order, has been, or is being, complied with; and
- (j) in the case of an application for an international production order that is in respect of one or more individual message/call application services—information that would be likely to be obtained by intercepting, under an order issued under this clause, messages sent or received, voice calls made or received, or video calls made or received, using those individual message/call application services would be likely to substantially assist in connection with:
 - (i) achieving a Part 5.3 object; or
 - (ii) determining whether the Part 5.3 supervisory order, or any succeeding Part 5.3 supervisory order, has been, or is being, complied with;

the eligible Judge or nominated AAT member may issue an order (to be known as an ***international production order***) directing the prescribed communications provider to:

- (k) in the case of an application for an international production order that is in respect of one or more individual transmission services:
 - (i) intercept communications carried by those individual transmission services during a specified period; and

- (ii) make those intercepted communications available to the Part 5.3 IPO agency; and
 - (iii) disclose to the Part 5.3 IPO agency specified telecommunications data that relates to those intercepted communications; and
 - (iv) disclose to the Part 5.3 IPO agency specified telecommunications data that relates to those individual transmission services; or
- (1) in the case of an application for an international production order that is in respect of one or more individual message/call application services:
- (i) intercept messages sent or received, voice calls made or received, or video calls made or received, using those individual message/call application services during a specified period; and
 - (ii) make those intercepted messages, voice calls or video calls available to the Part 5.3 IPO agency; and
 - (iii) disclose to the Part 5.3 IPO agency specified telecommunications data that relates to those intercepted messages, voice calls or video calls; and
 - (iv) disclose to the Part 5.3 IPO agency specified telecommunications data that relates to those individual message/call application services.

Note 1: Part 5.3 of the *Criminal Code* creates offences relating to terrorist acts.

Note 2: Part 5.5 of the *Criminal Code* creates offences relating to engaging in a hostile activity in a foreign country.

Note 3: Sections 104.27 and 105A.18A of the *Criminal Code* create offences for contravening Part 5.3 supervisory orders.

Note 4: Subclauses (7) and (8) restrict the issuing of international production orders if subparagraph (2)(g)(ii) or (h)(ii) applies.

Period specified in international production order

- (3) A period specified in an international production order for the purposes of subparagraph (2)(k)(i) or (1)(i) must not begin before

Schedule 1 International production orders

Part 3 International production orders relating to Part 5.3 supervisory orders

Division 2 International production orders relating to interception: Part 5.3 supervisory orders

Clause 60

the time when the order is given to the prescribed communications provider.

Note: International production orders are given under clause 111.

- (4) The period specified in an international production order for the purposes of subparagraph (2)(k)(i) or (l)(i) must not be longer than:
- (a) if subparagraph (2)(g)(ii) or (h)(ii) applies (as the case requires)—45 days; or
 - (b) otherwise—90 days.

Matters to which eligible Judge or nominated AAT member must have regard

- (5) In deciding whether to issue an international production order under subclause (2) (in the case of an application for an international production order that is in respect of one or more individual transmission services), the eligible Judge or nominated AAT member must have regard to the following matters:
- (a) how much the privacy of any person or persons would be likely to be interfered with by intercepting, under an international production order, communications that are being carried by those individual transmission services;
 - (b) how much the information referred to in paragraph (2)(i) would be likely to assist in connection with:
 - (i) achieving a Part 5.3 object; or
 - (ii) determining whether the Part 5.3 supervisory order, or any succeeding Part 5.3 supervisory order, has been, or is being, complied with;
 - (c) to what extent methods for:
 - (i) achieving a Part 5.3 object; or
 - (ii) determining whether the Part 5.3 supervisory order, or any succeeding Part 5.3 supervisory order, has been, or is being, complied with;that do not involve so intercepting communications have been used by, or are available to, the agency;

- (d) how much the use of such methods would be likely to assist in connection with:
 - (i) achieving a Part 5.3 object; or
 - (ii) determining whether the Part 5.3 supervisory order, or any succeeding Part 5.3 supervisory order, has been, or is being, complied with;
- (e) how much the use of such methods would be likely to prejudice:
 - (i) achieving a Part 5.3 object; or
 - (ii) determining whether the Part 5.3 supervisory order, or any succeeding Part 5.3 supervisory order, has been, or is being, complied with;whether because of delay or for any other reason;
- (f) whether intercepting, under an international production order, communications carried by those individual transmission services would be the method that is likely to have the least interference with any person's privacy;
- (g) in relation to a Part 5.3 supervisory order that is a control order—the possibility that the person in relation to whom the control order is in force:
 - (i) has engaged, is engaging, or will engage, in a terrorist act; or
 - (ii) has provided, is providing, or will provide, support for a terrorist act; or
 - (iii) has facilitated, is facilitating, or will facilitate, a terrorist act; or
 - (iv) has provided, is providing, or will provide, support for the engagement in a hostile activity in a foreign country; or
 - (v) has facilitated, is facilitating, or will facilitate, the engagement in a hostile activity in a foreign country;
- (ga) in relation to a Part 5.3 supervisory order that is an extended supervision order or an interim supervision order—the possibility that the person in relation to whom the order is in force has committed, is committing, or will commit, a serious Part 5.3 offence;

Schedule 1 International production orders

Part 3 International production orders relating to Part 5.3 supervisory orders

Division 2 International production orders relating to interception: Part 5.3 supervisory orders

Clause 60

- (gb) in relation to any Part 5.3 supervisory order—the possibility that the person in relation to whom the Part 5.3 supervisory order is in force:
 - (i) has contravened, is contravening, or will contravene, the Part 5.3 supervisory order; or
 - (ii) will contravene a succeeding Part 5.3 supervisory order;
 - (h) in relation to an application by a Part 5.3 IPO agency of Victoria—any submissions made by a Victorian PIM under clause 58 to the eligible Judge or nominated AAT member;
 - (i) in relation to an application by a Part 5.3 IPO agency of Queensland—any submissions made by a Queensland PIM under clause 59 to the eligible Judge or nominated AAT member;
 - (j) such other matters (if any) as the eligible Judge or nominated AAT member considers relevant.
- (6) In deciding whether to issue an international production order under subclause (2) (in the case of an application for an international production order that is in respect of one or more individual message/call application services), the eligible Judge or nominated AAT member must have regard to the following matters:
- (a) how much the privacy of any person or persons would be likely to be interfered with by intercepting, under an international production order, messages sent or received, voice calls made or received, or video calls made or received, using those individual message/call application services;
 - (b) how much the information referred to in paragraph (2)(j) would be likely to assist in connection with:
 - (i) achieving a Part 5.3 object; or
 - (ii) determining whether the Part 5.3 supervisory order, or any succeeding Part 5.3 supervisory order, has been, or is being, complied with;
 - (c) to what extent methods for:
 - (i) achieving a Part 5.3 object; or

- (ii) determining whether the Part 5.3 supervisory order, or any succeeding Part 5.3 supervisory order, has been, or is being, complied with;
that do not involve so intercepting messages, voice calls or video calls have been used by, or are available to, the agency;
- (d) how much the use of such methods would be likely to assist in connection with:
 - (i) achieving a Part 5.3 object; or
 - (ii) determining whether the Part 5.3 supervisory order, or any succeeding Part 5.3 supervisory order, has been, or is being, complied with;
- (e) how much the use of such methods would be likely to prejudice:
 - (i) achieving a Part 5.3 object; or
 - (ii) determining whether the Part 5.3 supervisory order, or any succeeding Part 5.3 supervisory order, has been, or is being, complied with;
whether because of delay or for any other reason;
- (f) whether intercepting, under an international production order, messages sent or received, voice calls made or received, or video calls made or received, using those individual message/call application services would be the method that is likely to have the least interference with any person's privacy;
- (g) in relation to a Part 5.3 supervisory order that is a control order—the possibility that the person in relation to whom the control order is in force:
 - (i) has engaged, is engaging, or will engage, in a terrorist act; or
 - (ii) has provided, is providing, or will provide, support for a terrorist act; or
 - (iii) has facilitated, is facilitating, or will facilitate, a terrorist act; or
 - (iv) has provided, is providing, or will provide, support for the engagement in a hostile activity in a foreign country; or

Schedule 1 International production orders

Part 3 International production orders relating to Part 5.3 supervisory orders

Division 2 International production orders relating to interception: Part 5.3 supervisory orders

Clause 60

- (v) has facilitated, is facilitating, or will facilitate, the engagement in a hostile activity in a foreign country;
- (ga) in relation to a Part 5.3 supervisory order that is an extended supervision order or an interim supervision order—the possibility that the person in relation to whom the order is in force has committed, is committing, or will commit, a serious Part 5.3 offence;
- (gb) in relation to any Part 5.3 supervisory order—the possibility that the person in relation to whom the Part 5.3 supervisory order is in force:
 - (i) has contravened, is contravening, or will contravene, the Part 5.3 supervisory order; or
 - (ii) will contravene a succeeding Part 5.3 supervisory order;
- (h) in relation to an application by a Part 5.3 IPO agency of Victoria—any submissions made by a Victorian PIM under clause 58 to the eligible Judge or nominated AAT member; and
- (i) in relation to an application by a Part 5.3 IPO agency of Queensland—any submissions made by a Queensland PIM under clause 59 to the eligible Judge or nominated AAT member;
- (j) such other matters (if any) as the eligible Judge or nominated AAT member considers relevant.

Restriction on issuing order

- (7) The eligible Judge or nominated AAT member must not issue an international production order under subclause (2) in a case where subparagraph (2)(g)(ii) applies, unless the eligible Judge or nominated AAT member is satisfied that:
 - (a) the Part 5.3 IPO agency has exhausted all other practicable methods of identifying the individual transmission services used, or likely to be used, by the person to whom the Part 5.3 supervisory order referred to in subparagraph (2)(g)(ii) relates; or

- (b) interception of communications carried by individual transmission services used or likely to be used by that person would not otherwise be possible.
- (8) The eligible Judge or nominated AAT member must not issue an international production order under subclause (2) in a case where: subparagraph (2)(h)(ii) applies, unless the eligible Judge or nominated AAT member is satisfied that:
 - (a) the Part 5.3 IPO agency has exhausted all other practicable methods of identifying the individual message/call application services used, or likely to be used, by the person the person to whom the Part 5.3 supervisory order referred to in subparagraph (2)(h)(ii) relates; or
 - (b) interception of messages sent or received, voice calls made or received, or video calls made or received, using individual message/call application services used or likely to be used by that person would not otherwise be possible.

61 Content of international production order

Scope

- (1) This clause applies to an international production order issued under clause 60 in response to an application made by a Part 5.3 IPO agency.

Content

- (2) The order must be signed by the eligible Judge or nominated AAT member who issued it.
- (3) The order must set out the following:
 - (a) the date on which the order was issued;
 - (b) the name of the Part 5.3 IPO agency;
 - (c) the name of the prescribed communications provider to whom the order is directed;
 - (d) the name of the designated international agreement nominated in the application for the order;

Schedule 1 International production orders

Part 3 International production orders relating to Part 5.3 supervisory orders

Division 2 International production orders relating to interception: Part 5.3 supervisory orders

Clause 61

- (e) the applicable telecommunications identifiers:
 - (i) in the case of an order that is in respect of one or more individual transmission services—to which those individual transmission services relate; or
 - (ii) in the case of an order that is in respect of one or more individual message/call application services—to which those individual message/call application services relate;
 - (f) a statement to the effect that the order is issued on the basis of a Part 5.3 supervisory order made in relation to a person;
 - (g) the name of the person;
 - (h) a statement to the effect that the Part 5.3 supervisory order is:
 - (i) an interim control order; or
 - (ii) a confirmed control order; or
 - (iii) an interim supervision order; or
 - (iv) an extended supervision order.
- (4) If the order directs a prescribed communications provider to intercept communications, the order may require the provider to:
- (a) intercept those communications in a specified way; and
 - (b) make those intercepted communications available to the Part 5.3 IPO agency in a specified way.
- (5) A requirement under subclause (4) may:
- (a) require that intercepted communications be made available to the Part 5.3 IPO agency directly; or
 - (b) require that intercepted communications be made available to the Part 5.3 IPO agency indirectly via the Australian Designated Authority.
- (6) If the order directs a prescribed communications provider to intercept messages, voice calls or video calls, the order may require the provider to:
- (a) intercept those messages, voice calls or video calls in a specified way; and

- (b) make those intercepted messages, voice calls or video calls available to the Part 5.3 IPO agency in a specified way.
- (7) A requirement under subclause (6) may:
 - (a) require that intercepted messages, voice calls or video calls be made available to the Part 5.3 IPO agency directly; or
 - (b) require that intercepted messages, voice calls or video calls be made available to the Part 5.3 IPO agency indirectly via the Australian Designated Authority.
- (8) If the order directs a prescribed communications provider to disclose telecommunications data to the Part 5.3 IPO agency, the order may require the provider to disclose that data to the agency in a specified way.
- (9) A requirement under subclause (8) may:
 - (a) require that the telecommunications data be disclosed to the Part 5.3 IPO agency directly; or
 - (b) require that the telecommunications data be disclosed to the Part 5.3 IPO agency indirectly via the Australian Designated Authority.
- (10) For the purposes of this clause, a specified way may deal with matters of timing.

Example: A requirement under subclause (4) may require that an intercepted communication be made available to the Part 5.3 IPO agency within 30 minutes after the communication was completed.

62 Issue of further international production order

- (1) If:
 - (a) an international production order (the *original order*) was issued under clause 60; and
 - (b) the original order was in respect of one or more individual transmission services; and
 - (c) the original order was directed to a prescribed communications provider;

Schedule 1 International production orders

Part 3 International production orders relating to Part 5.3 supervisory orders

Division 2 International production orders relating to interception: Part 5.3 supervisory orders

Clause 62

this Schedule does not prevent the issue of a further international production order under clause 60 that is:

- (d) in respect of any or all of those services; and
- (e) directed to the provider;

so long as the period specified in the further order for the purposes of subparagraph 60(2)(k)(i) of this Schedule begins after the end of the period specified in the original order for the purposes of that subparagraph.

(2) If:

- (a) an international production order (the *original order*) was issued under clause 60; and
- (b) the original order was in respect of one or more individual message/call application services; and
- (c) the original order was directed to a prescribed communications provider;

this Schedule does not prevent the issue of a further international production order under clause 60 that is:

- (d) in respect of any or all of those services; and
- (e) directed to the provider;

so long as the period specified in the further order for the purposes of subparagraph 60(2)(l)(i) of this Schedule begins after the end of the period specified in the original order for the purposes of that subparagraph.

Division 3—International production orders relating to stored communications: Part 5.3 supervisory orders

Subdivision A—Applications

63 Application for international production order—Part 5.3 supervisory order

- (1) A Part 5.3 IPO agency may apply to an issuing authority for an international production order under clause 69 that:
 - (a) is in respect of a particular person; and
 - (b) is directed to a prescribed communications provider.
- (2) The application must nominate a designated international agreement.
- (3) The application must be made on the Part 5.3 IPO agency's behalf by:
 - (a) if the agency is referred to in subclause 22(3)—a person referred to in that subclause in relation to the agency; or
 - (b) otherwise:
 - (i) the chief officer of the agency; or
 - (ii) an officer of the agency (by whatever name called) who holds, or is acting in, an office or position in the agency nominated under subclause (4).
- (4) The chief officer of the Part 5.3 IPO agency may, in writing, nominate for the purposes of subparagraph (3)(b)(ii) an office or position in the agency that is involved in the management of the agency.
- (5) A nomination under subclause (4) is not a legislative instrument.

Schedule 1 International production orders

Part 3 International production orders relating to Part 5.3 supervisory orders

Division 3 International production orders relating to stored communications: Part 5.3 supervisory orders

Clause 64

64 Form of application

- (1) An application under clause 63 must be in writing.
- (2) However, a person making the application on the Part 5.3 IPO agency's behalf may make the application by telephone if the person:
 - (a) is the chief officer of the agency or a person in relation to whom an authorisation by the chief officer is in force under subclause (3); and
 - (b) thinks it necessary, because of urgent circumstances, to make the application by telephone.

Note: See also clause 17A (urgent circumstances) and clause 172 (action required).

- (3) The chief officer of a Part 5.3 IPO agency may, in writing, authorise persons (including classes of persons) for the purposes of subclause (2). However, each person must be entitled under clause 63 to make applications on the agency's behalf.

65 Contents of written application

An application under clause 63 must, if it is in writing, set out:

- (a) the name of the Part 5.3 IPO agency; and
- (b) the name of the person making the application on the agency's behalf.

66 Affidavits to accompany written application

- (1) An application under clause 63 must, if it is in writing, be accompanied by an affidavit complying with this clause.
- (2) The affidavit must set out the facts and other grounds on which the application is based.
- (3) Despite subclause (1), a written application may be accompanied by 2 or more affidavits that together set out each matter that, apart from this subclause, this clause would have required an affidavit accompanying the application to set out.

67 Information to be given on telephone application

The information given to an issuing authority in connection with a telephone application under clause 63 to the issuing authority:

- (a) must include particulars of the urgent circumstances because of which the person making the application on the Part 5.3 IPO agency's behalf thinks it necessary to make the application by telephone; and
- (b) must include each matter that, if the application had been made in writing, clause 65 or 66 would have required the application, or an affidavit accompanying it, to set out; and
- (c) must be given orally or in writing, as the issuing authority directs.

68 Giving further information to issuing authority

- (1) An issuing authority may require further information to be given in connection with an application under clause 63 to the issuing authority for an international production order.
- (2) The further information:
 - (a) must be given on oath if the application was made in writing; and
 - (b) must be given orally or otherwise, as the issuing authority directs.

Subdivision B—International production orders relating to stored communications

69 Issue of international production order—Part 5.3 supervisory order

Scope

- (1) This clause applies if a Part 5.3 IPO agency applies, under clause 63, to an issuing authority for an international production order that:

Schedule 1 International production orders

Part 3 International production orders relating to Part 5.3 supervisory orders

Division 3 International production orders relating to stored communications: Part 5.3 supervisory orders

Clause 69

- (a) is in respect of a particular person (the *relevant person*); and
- (b) is directed to a prescribed communications provider.

Issue of international production order

- (2) If the issuing authority is satisfied, on the basis of the information given to the issuing authority under this Division in connection with the application, that:
 - (a) a Part 5.3 supervisory order is in force in relation to the relevant person; and
 - (b) there are reasonable grounds for suspecting that the prescribed communications provider holds any of the following stored communications:
 - (i) stored communications that consist of communications that the relevant person has made using a telecommunications network owned or operated by the prescribed communications provider;
 - (ii) stored communications that consist of communications that another person has made using a telecommunications network owned or operated by the prescribed communications provider, and for which the relevant person is the intended recipient;
 - (iii) stored communications that consist of communications that the relevant person has made using a transmission service supplied by the prescribed communications provider;
 - (iv) stored communications that consist of communications that another person has made using a transmission service supplied by the prescribed communications provider, and for which the relevant person is the intended recipient;
 - (v) stored communications that consist of messages that the relevant person has sent or received using a message/call application service provided by the prescribed communications provider;
 - (vi) stored communications that consist of recordings of voice calls that the relevant person has made or received

- using a message/call application service provided by the prescribed communications provider;
- (vii) stored communications that consist of recordings of video calls that the relevant person has made or received using a message/call application service provided by the prescribed communications provider;
 - (viii) stored communications that consist of material that the relevant person has uploaded for storage or back-up by a storage/back-up service provided by the prescribed communications provider;
 - (ix) stored communications that consist of material that the relevant person has posted to a general electronic content service provided by the prescribed communications provider; and
- (ba) the person who made the application on behalf of the agency reasonably suspects that the prescribed communications provider is based in, or operates in, a foreign country that is a party to the designated international agreement nominated in the application; and
- (c) Subdivision A has been complied with in relation to the application; and
- (d) in the case of a telephone application—because of urgent circumstances, it was necessary to make the application by telephone; and
- (e) information that would be likely to be obtained by making a copy, under an order issued under this clause, of the stored communications would be likely to substantially assist in connection with:
- (i) achieving a Part 5.3 object; or
 - (ii) determining whether the Part 5.3 supervisory order has been, or is being, complied with;
- the issuing authority may issue an order (to be known as an ***international production order***) directing the prescribed communications provider to:
- (f) make a copy of any such stored communications; and
 - (g) make the copy available to the Part 5.3 IPO agency; and

Schedule 1 International production orders

Part 3 International production orders relating to Part 5.3 supervisory orders

Division 3 International production orders relating to stored communications: Part 5.3 supervisory orders

Clause 69

- (h) if the stored communications consist of communications carried by an individual transmission service—disclose to the agency:
 - (i) specified telecommunications data that relates to those communications; and
 - (ii) specified telecommunications data that relates to the individual transmission service; and
 - (i) if the stored communications consist of messages sent or received using an individual message/call application service—disclose to the agency:
 - (i) specified telecommunications data that relates to those messages; and
 - (ii) specified telecommunications data that relates to the individual message/call application service; or
 - (j) if the stored communications consist of recordings of voice calls made or received using an individual message/call application service—disclose to the agency:
 - (i) specified telecommunications data that relates to those voice calls; and
 - (ii) specified telecommunications data that relates to the individual message/call application service; and
 - (k) if the stored communications consist of recordings of video calls made or received using an individual message/call application service—disclose to the agency:
 - (i) specified telecommunications data that relates to those video calls; and
 - (ii) specified telecommunications data that relates to the individual message/call application service; and
 - (l) if the stored communications consist of material that has been uploaded by an end-user for storage or back-up by a storage/back-up service—disclose to the agency:
 - (i) specified telecommunications data that relates to that material; and
 - (ii) specified telecommunications data that relates to the end-user’s account with the storage/back-up service; and
-

- (m) if the stored communications consist of material posted to a general electronic content service by an end-user—disclose to the agency:
 - (i) specified telecommunications data that relates to that material; and
 - (ii) specified telecommunications data that relates to the end-user's account with the general electronic content service.

Matters to which issuing authority must have regard

- (3) In deciding whether to issue an international production order under subclause (2), the issuing authority must have regard to the following matters:
 - (a) how much the privacy of any person or persons would be likely to be interfered with by the Part 5.3 IPO agency obtaining, under an international production order, a copy of the stored communications;
 - (b) how much the information mentioned in paragraph (2)(e) would be likely to assist in connection with:
 - (i) achieving a Part 5.3 object; or
 - (ii) determining whether the Part 5.3 supervisory order has been, or is being, complied with;
 - (c) to what extent methods for:
 - (i) achieving a Part 5.3 object; or
 - (ii) determining whether the Part 5.3 supervisory order has been, or is being, complied with;that do not involve so obtaining a copy of the stored communications have been used by, or are available to, the Part 5.3 IPO agency;
 - (d) how much the use of such methods would be likely to assist in connection with:
 - (i) achieving a Part 5.3 object; or
 - (ii) determining whether the Part 5.3 supervisory order has been, or is being, complied with;

Schedule 1 International production orders

Part 3 International production orders relating to Part 5.3 supervisory orders

Division 3 International production orders relating to stored communications: Part 5.3 supervisory orders

Clause 70

- (e) how much the use of such methods would be likely to prejudice:
 - (i) achieving a Part 5.3 object; or
 - (ii) determining whether the Part 5.3 supervisory order has been, or is being, complied with; whether because of delay or for any other reason;
- (f) such other matters (if any) as the issuing authority considers relevant.

70 Content of international production order

Scope

- (1) This clause applies to an international production order issued under clause 69 in response to an application made by a Part 5.3 IPO agency.

Content

- (2) The order must be signed by the issuing authority who issued it.
- (3) The order must set out the following:
 - (a) the date on which the order was issued;
 - (b) the name of the Part 5.3 IPO agency;
 - (c) the name of the prescribed communications provider to whom the order is directed;
 - (d) the name of the designated international agreement nominated in the application for the order;
 - (e) a statement to the effect that the order is issued on the basis of a Part 5.3 supervisory order made in relation to a person;
 - (f) the name of the person;
 - (g) a statement to the effect that the Part 5.3 supervisory order is:
 - (i) an interim control order; or
 - (ii) a confirmed control order; or
 - (iii) an interim supervision order; or
 - (iv) an extended supervision order.

- (4) If the order directs a prescribed communications provider to make a copy of stored communications available to the Part 5.3 IPO agency, the order may require the provider to make that copy available to the agency in a specified way.
- (5) A requirement under subclause (4) may:
 - (a) require that a copy of stored communications be made available to the Part 5.3 IPO agency directly; or
 - (b) require that a copy of stored communications be made available to the Part 5.3 IPO agency indirectly via the Australian Designated Authority.
- (6) If the order directs a prescribed communications provider to disclose telecommunications data to the Part 5.3 IPO agency, the order may require the provider to disclose that data to the agency in a specified way.
- (7) A requirement under subclause (6) may:
 - (a) require that the telecommunications data be disclosed to the Part 5.3 IPO agency directly; or
 - (b) require that the telecommunications data be disclosed to the Part 5.3 IPO agency indirectly via the Australian Designated Authority.
- (8) For the purposes of this clause, a specified way may deal with matters of timing.

71 Issue of further international production order

If:

- (a) an international production order (the *original order*) was issued under clause 69; and
- (b) the original order was in respect of a particular person; and
- (c) the original order was directed to a prescribed communications provider;

this Schedule does not prevent the issue of a further international production order under clause 69 that:

- (d) is in respect of the person; and

Schedule 1 International production orders

Part 3 International production orders relating to Part 5.3 supervisory orders

Division 3 International production orders relating to stored communications: Part 5.3 supervisory orders

Clause 71

(e) is directed to the provider.

Division 4—International production orders relating to telecommunications data: Part 5.3 supervisory orders

Subdivision A—Applications

72 Application for international production order—Part 5.3 supervisory order

- (1) A Part 5.3 IPO agency may apply to an issuing authority for an international production order under clause 78 that:
 - (a) is in respect of a particular person; and
 - (b) is directed to a prescribed communications provider.
- (2) The application must nominate a designated international agreement.
- (3) The application must be made on the Part 5.3 IPO agency's behalf by an authorised officer of the agency.

73 Form of application

- (1) An application under clause 72 must be in writing.
- (2) However, a person making the application on the Part 5.3 IPO agency's behalf may make the application by telephone if the person:
 - (a) is the chief officer of the agency or a person in relation to whom an authorisation by the chief officer is in force under subclause (3); and
 - (b) thinks it necessary, because of urgent circumstances, to make the application by telephone.

Note: See also clause 17A (urgent circumstances) and clause 172 (action required).

Schedule 1 International production orders

Part 3 International production orders relating to Part 5.3 supervisory orders

Division 4 International production orders relating to telecommunications data: Part 5.3 supervisory orders

Clause 74

- (3) The chief officer of a Part 5.3 IPO agency may, in writing, authorise persons (including classes of persons) for the purposes of subclause (2). However, each person must be entitled under clause 72 to make applications on the agency's behalf.

74 Contents of written application

An application under clause 72 must, if it is in writing, set out:

- (a) the name of the Part 5.3 IPO agency; and
- (b) the name of the person making the application on the agency's behalf.

75 Affidavits to accompany written application

- (1) An application under clause 72 must, if it is in writing, be accompanied by an affidavit complying with this clause.
- (2) The affidavit must set out the facts and other grounds on which the application is based.
- (3) Despite subclause (1), a written application may be accompanied by 2 or more affidavits that together set out each matter that, apart from this subclause, this clause would have required an affidavit accompanying the application to set out.

76 Information to be given on telephone application

The information given to an issuing authority in connection with a telephone application under clause 72 to the issuing authority:

- (a) must include particulars of the urgent circumstances because of which the person making the application on the Part 5.3 IPO agency's behalf thinks it necessary to make the application by telephone; and
- (b) must include each matter that, if the application had been made in writing, clause 74 or 75 would have required the application, or an affidavit accompanying it, to set out; and
- (c) must be given orally or in writing, as the issuing authority directs.

77 Giving further information to issuing authority

- (1) An issuing authority may require further information to be given in connection with an application under clause 72 to the issuing authority for an international production order.
- (2) The further information:
 - (a) must be given on oath if the application was made in writing; and
 - (b) must be given orally or otherwise, as the issuing authority directs.

Subdivision B—International production orders relating to telecommunications data

78 Issue of international production order—Part 5.3 supervisory order

Scope

- (1) This clause applies if a Part 5.3 IPO agency applies, under clause 72, to an issuing authority for an international production order that:
 - (a) is in respect of a particular person (the *relevant person*); and
 - (b) is directed to a prescribed communications provider.

Issue of international production order

- (2) If the issuing authority is satisfied, on the basis of the information given to the issuing authority under this Division in connection with the application, that:
 - (a) a Part 5.3 supervisory order is in force in relation to the relevant person; and
 - (b) there are reasonable grounds for suspecting that the prescribed communications provider holds, or is likely to commence to hold, any of the following telecommunications data:

Schedule 1 International production orders

Part 3 International production orders relating to Part 5.3 supervisory orders

Division 4 International production orders relating to telecommunications data: Part 5.3 supervisory orders

Clause 78

- (i) telecommunications data that relates to communications that the relevant person has made using an individual transmission service supplied by the prescribed communications provider;
- (ii) telecommunications data that relates to an individual transmission service supplied using a telecommunications network owned or operated by the prescribed communications provider, where the individual transmission service is used, or is likely to be used, by the relevant person;
- (iii) telecommunications data that relates to an individual transmission service supplied by the prescribed communications provider, where the individual transmission service is used, or is likely to be used, by the relevant person;
- (iv) telecommunications data that relates to messages sent or received by the relevant person using an individual message/call application service provided by the prescribed communications provider;
- (v) telecommunications data that relates to voice calls made or received by the relevant person using an individual message/call application service provided by the prescribed communications provider;
- (vi) telecommunications data that relates to video calls made or received by the relevant person using an individual message/call application service provided by the prescribed communications provider;
- (vii) telecommunications data that relates to an individual message/call application service provided by the prescribed communications provider, where the individual message/call application service is used, or is likely to be used, by the relevant person;
- (viii) telecommunications data that relates to material that has been uploaded by the relevant person for storage or back-up by a storage/back-up service provided by the prescribed communications provider;

- (ix) telecommunications data that relates to material that has been posted by the relevant person on a general electronic content service provided by the prescribed communications provider; and
- (ba) the person who made the application on behalf of the agency reasonably suspects that the prescribed communications provider is based in, or operates in, a foreign country that is a party to the designated international agreement nominated in the application; and
- (c) Subdivision A has been complied with in relation to the application; and
- (d) in the case of a telephone application—because of urgent circumstances, it was necessary to make the application by telephone; and
- (e) disclosing the telecommunications data to the agency, under an order issued under this clause, would be likely to substantially assist in connection with:
 - (i) achieving a Part 5.3 object; or
 - (ii) determining whether the Part 5.3 supervisory order, or any succeeding Part 5.3 supervisory order, has been, or is being, complied with;

the issuing authority may issue an order (to be known as an ***international production order***) directing the prescribed communications provider to do either or both of the following:

- (f) so far as the telecommunications data is held by the prescribed communications provider when the international production order comes into force—disclose any such telecommunications data to the agency;
- (g) so far as the telecommunications data commences to be held by the prescribed communications provider during a specified period—disclose any such telecommunications data to the agency.

Schedule 1 International production orders

Part 3 International production orders relating to Part 5.3 supervisory orders

Division 4 International production orders relating to telecommunications data: Part 5.3 supervisory orders

Clause 78

Period specified in international production order

- (3) A period specified in an international production order for the purposes of paragraph (2)(g) must not begin before the time when the order is given to the prescribed communications provider.

Note: International production orders are given under clause 111.

- (4) A period specified in an international production order for the purposes of paragraph (2)(g) must not be longer than 90 days.
- (5) In deciding whether to issue an international production order under subclause (2), the issuing authority must have regard to the following matters:
- (a) how much the privacy of any person or persons would be likely to be interfered with by obtaining, under an international production order, the telecommunications data;
 - (b) how much the telecommunications data would be likely to assist in connection with:
 - (i) achieving a Part 5.3 object; or
 - (ii) determining whether the Part 5.3 supervisory order, or any succeeding Part 5.3 supervisory order, has been, or is being, complied with;
 - (c) to what extent methods for:
 - (i) achieving a Part 5.3 object; or
 - (ii) determining whether the Part 5.3 supervisory order, or any succeeding Part 5.3 supervisory order, has been, or is being, complied with;that do not involve so obtaining the telecommunications data have been used by, or are available to, the Part 5.3 IPO agency;
 - (d) how much the use of such methods would be likely to assist in connection with:
 - (i) achieving a Part 5.3 object; or
 - (ii) determining whether the Part 5.3 supervisory order, or any succeeding Part 5.3 supervisory order, has been, or is being, complied with;

- (e) how much the use of such methods would be likely to prejudice:
 - (i) achieving a Part 5.3 object; or
 - (ii) determining whether the Part 5.3 supervisory order, or any succeeding Part 5.3 supervisory order, has been, or is being, complied with;
whether because of delay or for any other reason;
- (f) such other matters (if any) as the issuing authority considers relevant.

79 Content of international production order

Scope

- (1) This clause applies to an international production order issued under clause 78 in response to an application made by a Part 5.3 IPO agency.

Content

- (2) The order must be signed by the issuing authority who issued it.
- (3) The order must set out the following:
 - (a) the date on which the order was issued;
 - (b) the name of the Part 5.3 IPO agency;
 - (c) the name of the prescribed communications provider to whom the order is directed;
 - (d) the name of the designated international agreement nominated in the application for the order;
 - (e) a statement to the effect that the order is issued on the basis of a Part 5.3 supervisory order made in relation to a person;
 - (f) the name of the person;
 - (g) a statement to the effect that the Part 5.3 supervisory order is:
 - (i) an interim control order; or
 - (ii) a confirmed control order; or
 - (iii) an interim supervision order; or

Schedule 1 International production orders

Part 3 International production orders relating to Part 5.3 supervisory orders

Division 4 International production orders relating to telecommunications data: Part 5.3 supervisory orders

Clause 80

(iv) an extended supervision order.

- (4) If the order directs a prescribed communications provider to disclose telecommunications data to the Part 5.3 IPO agency, the order may require the provider to disclose that data to the agency in a specified way.
- (5) A requirement under subclause (4) may:
- (a) require that the telecommunications data be disclosed to the Part 5.3 IPO agency directly; or
 - (b) require that the telecommunications data be disclosed to the Part 5.3 IPO agency indirectly via the Australian Designated Authority.
- (6) For the purposes of this clause, a specified way may deal with matters of timing.

Example: If a requirement under subclause (4) relates to telecommunications data that commences to be held by a prescribed communications provider during a specified period, the requirement may require that the telecommunications data be disclosed to the Part 5.3 IPO agency within 30 minutes after the telecommunications data commences to be held.

80 Issue of further international production order

If:

- (a) an international production order (the *original order*) was issued under clause 78; and
- (b) the original order was in respect of a particular person; and
- (c) the original order was directed to a prescribed communications provider;

this Schedule does not prevent the issue of a further international production order under clause 78 that:

- (d) is in respect of the person; and
- (e) is directed to the provider.

Division 5—Notification to Ombudsman by Part 5.3 IPO agencies in relation to international production orders

81 Notification to Ombudsman by Part 5.3 IPO agencies in relation to international production orders

- (1) Within 3 months after an international production order is issued under this Part in response to an application by a Part 5.3 IPO agency, the chief officer of the agency must:
 - (a) notify the Ombudsman that the order has been issued; and
 - (b) give to the Ombudsman a copy of the order.
- (2) If the chief officer of a Part 5.3 IPO agency contravenes paragraph 114(1)(d) of this Schedule (so far as that paragraph relates to an international production order issued under this Part), the chief officer must:
 - (a) notify the Ombudsman of the contravention; and
 - (b) do so as soon as practicable after the contravention.
- (3) A failure to comply with subclause (1) or (2) does not affect the validity of an international production order.

Part 4—International production orders relating to national security

Division 1—Introduction

82 Simplified outline of this Part

- International production orders may be issued for purposes in connection with the carrying out by the Organisation of its functions.
- There are 3 types of international production orders:
 - (a) international production orders relating to interception; and
 - (b) international production orders relating to stored communications; and
 - (c) international production orders relating to telecommunications data.
- An international production order is directed to a prescribed communications provider.
- An international production order may be issued in response to an application made by the Organisation.
- An application for an international production order must nominate a designated international agreement.

Note: An international production order comes into force when it is given to a prescribed communications provider under clause 112.

Division 2—International production orders relating to interception: national security

Subdivision A—Applications

83 Application for international production order—national security

- (1) The Organisation may apply to a nominated AAT Security Division member for an international production order under clause 89 that:
 - (a) is in respect of:
 - (i) one or more individual transmission services; or
 - (ii) one or more individual message/call application services; and
 - (b) is directed to a prescribed communications provider.
- (2) The application must nominate a designated international agreement.
- (3) The application must be made on the Organisation's behalf by:
 - (a) the Director-General of Security; or
 - (b) a Deputy Director-General of Security; or
 - (c) a senior position-holder in relation to whom an authorisation is in force under subclause (4).
- (4) The Director-General of Security may authorise in writing, for the purposes of subclause (3), senior position-holders who, or classes of senior position-holders who, are entitled under subclause (1) to make applications on the Organisation's behalf.

Attorney-General's consent to the making of an application

- (5) The Organisation must not make an application under subclause (1) unless the Attorney-General has consented to the making of the application.

Schedule 1 International production orders

Part 4 International production orders relating to national security

Division 2 International production orders relating to interception: national security

Clause 83

- (6) The Attorney-General must not consent to the making of an application under subclause (1) for an international production order that is in respect of one or more individual transmission services unless the Attorney-General is satisfied that:
- (a) there are reasonable grounds for suspecting that those individual transmission services are being, or are likely to be:
 - (i) used by a person engaged in, or reasonably suspected of being engaged in, or of being likely to engage in, activities prejudicial to security; or
 - (ii) the means by which a person receives or sends a communication from or to another person who is engaged in, or reasonably suspected of being engaged in, or of being likely to engage in, activities prejudicial to security; or
 - (iii) used for purposes prejudicial to security; and
 - (b) information that would be likely to be obtained by intercepting, under an order issued in response to the application, communications that are being carried by those individual transmission services would be likely to assist the Organisation in carrying out its function of obtaining intelligence relating to security.
- (7) The Attorney-General must not consent to the making of an application under subclause (1) for an international production order that is in respect of one or more individual message/call application services unless the Attorney-General is satisfied that:
- (a) there are reasonable grounds for suspecting that those individual message/call application services are being, or are likely to be:
 - (i) used by a person engaged in, or reasonably suspected of being engaged in, or of being likely to engage in, activities prejudicial to security; or
 - (ii) the means by which a person receives or sends a message, or receives or makes a voice call or video call, from or to another person who is engaged in, or reasonably suspected of being engaged in, or of being likely to engage in, activities prejudicial to security; or

- (iii) used for purposes prejudicial to security; and
- (b) information that would be likely to be obtained by intercepting, under an order issued in response to the application, messages sent or received, voice calls made or received, or video calls made or received, using those individual message/call application services would be likely to assist the Organisation in carrying out its function of obtaining intelligence relating to security.

Form of Attorney-General's consent to the making of an application

- (8) Subject to subclause (9), a consent given by the Attorney-General under subclause (5) must be in writing.
 - (9) If the person who proposes to make an application under subclause (1) on the Organisation's behalf thinks it necessary, because of urgent circumstances, for the Attorney-General to consent orally to the making of the application:
 - (a) the person may request the Attorney-General to consent orally to the making of the application; and
 - (b) if the person makes such a request—the Attorney-General may consent orally to the making of the application.
- Note: See also clause 17A (urgent circumstances).
- (9A) At the same time as a request is made by a person under subclause (9), the person must inform the Attorney-General of the particulars of the urgent circumstances because of which the person thought it necessary for the Attorney-General to consent orally to the making of the application concerned.
 - (10) If, in response to a request made by a person under subclause (9), the Attorney-General consents orally to the making of an application, the person must:
 - (a) give the Attorney-General a written report that sets out:
 - (i) particulars of the urgent circumstances because of which the person thought it necessary for the Attorney-General to consent orally; and

Schedule 1 International production orders

Part 4 International production orders relating to national security

Division 2 International production orders relating to interception: national security

Clause 84

- (ii) whether the application was granted, withdrawn or refused; and
 - (b) do so within 3 working days after the day on which the application was granted, withdrawn or refused.
- (11) If, in response to a request made by a person under subclause (9), the Attorney-General consents orally to the making of an application, the Organisation must:
 - (a) give the Inspector-General of Intelligence and Security a copy of the relevant report under subclause (10); and
 - (b) do so within 3 working days after the day on which the application was granted, withdrawn or refused.

84 Form of application

- (1) Subject to subclause (2), an application under clause 83 for an international production order must be in writing.
- (2) If the person making an application under clause 83 for an international production order on the Organisation's behalf thinks it necessary, because of urgent circumstances, to make the application by telephone, the person may make the application by telephone.

Note: See also clause 17A (urgent circumstances) and clause 172 (action required).

85 Contents of application

A written application under clause 83 for an international production order must set out:

- (a) a statement to the effect that the application is made by the Organisation; and
- (b) the name of the person making the application on the Organisation's behalf.

86 Affidavits to accompany written application

- (1) A written application under clause 83 for an international production order must be accompanied by an affidavit complying with this clause.
- (2) The affidavit must set out the facts and other grounds on which the application is based.
- (3) If the application is for an international production order in respect of one or more individual transmission services, the affidavit must set out the following information, so far as it can be derived from the Organisation's records:
 - (a) the number of previous applications (if any) for international production orders that the Organisation has made under clause 83 in relation to those individual transmission services;
 - (b) the number of international production orders (if any) previously issued in response to such applications;
 - (c) particulars of the use made by the Organisation of intercepted communications made available to the Organisation under such orders.
- (4) If the application is for an international production order in respect of one or more individual message/call application services, the affidavit must set out the following information, so far as it can be derived from the Organisation's records:
 - (a) the number of previous applications (if any) for international production orders that the Organisation has made under clause 83 in relation to those individual message/call application services;
 - (b) the number of international production orders (if any) previously issued in response to such applications;
 - (c) particulars of the use made by the Organisation of intercepted messages, voice calls or video calls made available to the Organisation under such orders.

Schedule 1 International production orders

Part 4 International production orders relating to national security

Division 2 International production orders relating to interception: national security

Clause 87

- (5) Despite subclause (1), a written application may be accompanied by 2 or more affidavits that together set out each matter that, apart from this subclause, this clause would have required an affidavit accompanying the application to set out.

87 Information to be given on telephone application

The information given to a nominated AAT Security Division member in connection with a telephone application under clause 83 to the nominated AAT Security Division member:

- (a) must include particulars of the urgent circumstances because of which the person making the application on the Organisation's behalf thinks it necessary to make the application by telephone; and
- (b) must include each matter that, if the application had been made in writing, clause 85 or 86 would have required the application, or an affidavit accompanying it, to set out; and
- (c) must be given orally or in writing, as the nominated AAT Security Division member directs.

88 Giving further information to nominated AAT Security Division member

- (1) A nominated AAT Security Division member may require further information to be given in connection with an application under clause 83 to the nominated AAT Security Division member for an international production order.
- (2) The further information:
 - (a) must be given on oath if the application was made in writing; and
 - (b) must be given orally or otherwise, as the nominated AAT Security Division member directs.

Subdivision B—International production orders relating to interception

89 Issue of international production order—national security

Scope

- (1) This clause applies if the Organisation applies, under clause 83, to a nominated AAT Security Division member for an international production order that:
 - (a) is in respect of:
 - (i) one or more individual transmission services; or
 - (ii) one or more individual message/call application services; and
 - (b) is directed to a prescribed communications provider.

Issue of international production order

- (2) If the nominated AAT Security Division member is satisfied, on the basis of the information given to the nominated AAT Security Division member under this Division in connection with the application, that:
 - (a) in the case of an application for an international production order that is in respect of one or more individual transmission services—there are reasonable grounds for suspecting that:
 - (i) the prescribed communications provider owns or operates a telecommunications network that is, or is likely to be, used to supply those individual transmission services; or
 - (ii) the prescribed communications provider supplies those individual transmission services; and
 - (b) in the case of an application for an international production order that is in respect of one or more individual message/call application services—there are reasonable grounds for suspecting that the prescribed communications provider provides those individual message/call application services; and

Schedule 1 International production orders

Part 4 International production orders relating to national security

Division 2 International production orders relating to interception: national security

Clause 89

- (ba) the person who made the application on behalf of the Organisation reasonably suspects that the prescribed communications provider is based in, or operates in, a foreign country that is a party to the designated international agreement nominated in the application; and
- (c) Subdivision A has been complied with in relation to the application; and
- (d) in the case of a telephone application—because of urgent circumstances, it was necessary to make the application by telephone; and
- (e) in the case of an application for an international production order that is in respect of one or more individual transmission services—there are reasonable grounds for suspecting that those services are being, or are likely to be:
 - (i) used by a person engaged in, or reasonably suspected of being engaged in, or of being likely to engage in, activities prejudicial to security; or
 - (ii) the means by which a person receives or sends a communication from or to another person who is engaged in, or reasonably suspected of being engaged in, or of being likely to engage in, activities prejudicial to security; or
 - (iii) used for purposes prejudicial to security; and
- (f) in the case of an application for an international production order that is in respect of one or more individual message/call application services—there are reasonable grounds for suspecting that those services are being, or are likely to be:
 - (i) used by a person engaged in, or reasonably suspected of being engaged in, or of being likely to engage in, activities prejudicial to security; or
 - (ii) the means by which a person receives or sends a message, or receives or makes a voice call or video call, from or to another person who is engaged in, or reasonably suspected of being engaged in, or of being likely to engage in, activities prejudicial to security; or
 - (iii) used for purposes prejudicial to security; and

- (g) in the case of an application for an international production order that is in respect of one or more individual transmission services—there are reasonable grounds for suspecting that information that would be likely to be obtained by intercepting, under an order issued under this clause, communications that are being carried by those individual transmission services would be likely to assist the Organisation in carrying out its function of obtaining intelligence relating to security; and
- (h) in the case of an application for an international production order that is in respect of one or more individual message/call application services—there are reasonable grounds for suspecting that information that would be likely to be obtained by intercepting, under an order issued under this clause, messages sent or received, voice calls made or received, or video calls made or received, using those individual message/call application services would be likely to assist the Organisation in carrying out its function of obtaining intelligence relating to security;

the nominated AAT Security Division member may issue an order (to be known as an *international production order*) directing the prescribed communications provider to:

- (i) in the case of an application for an international production order that is in respect of one or more individual transmission services:
 - (i) intercept communications carried by those individual transmission services during a specified period; and
 - (ii) make those intercepted communications available to the Organisation; and
 - (iii) disclose to the Organisation specified telecommunications data that relates to those intercepted communications; and
 - (iv) disclose to the Organisation specified telecommunications data that relates to those individual transmission services; or

Schedule 1 International production orders

Part 4 International production orders relating to national security

Division 2 International production orders relating to interception: national security

Clause 89

- (j) in the case of an application for an international production order that is in respect of one or more individual message/call application services:
 - (i) intercept messages sent or received, voice calls made or received, or video calls made or received, using those individual message/call application services during a specified period; and
 - (ii) make those intercepted messages, voice calls or video calls available to the Organisation; and
 - (iii) disclose to the Organisation specified telecommunications data that relates to those intercepted messages, voice calls or video calls; and
 - (iv) disclose to the Organisation specified telecommunications data that relates to those individual message/call application services.

Note: Subclauses (6) and (7) restrict the issuing of international production orders if subparagraph (2)(e)(ii) or (f)(ii) applies.

Period specified in international production order

- (3) A period specified in an international production order for the purposes of subparagraph (2)(i)(i) or (j)(i) must not begin before the time when the order is given to the prescribed communications provider.

Note: International production orders are given under clause 112.

- (4) The period specified in an international production order for the purposes of subparagraph (2)(i)(i) or (j)(i) must not be longer than:
 - (a) if subparagraph (2)(e)(ii) or (f)(ii) applies (as the case requires)—3 months; or
 - (b) otherwise—6 months.

Matters to which nominated AAT Security Division member must have regard

- (5) In deciding whether to issue an international production order under subclause (2), the nominated AAT Security Division member must have regard to the following matters:

- (a) in the case of an application for an international production order that is in respect of one or more individual transmission services:
 - (i) to what extent methods of carrying out the Organisation's function of obtaining intelligence relating to security (so far as carrying out that function relates to the target) that are less intrusive than intercepting, under such an order, communications being carried by those individual transmission services have been used by, or are available to, the Organisation; and
 - (ii) how much the use of such methods would be likely to assist the Organisation in carrying out its function of obtaining intelligence relating to security (so far as carrying out that function relates to the target); and
 - (iii) how much the use of such methods would be likely to prejudice the Organisation in carrying out its function of obtaining intelligence relating to security (so far as carrying out that function relates to the target), whether because of delay or for any other reason; and
 - (iv) such other matters (if any) as the nominated AAT Security Division member considers relevant;
- (b) in the case of an application for an international production order that is in respect of one or more individual message/call application services:
 - (i) to what extent methods of carrying out the Organisation's function of obtaining intelligence relating to security (so far as carrying out that function relates to the target) that are less intrusive than intercepting, under such an order, messages sent or received, voice calls made or received, or video calls made or received, using those individual message/call application services have been used by, or are available to, the Organisation; and
 - (ii) how much the use of such methods would be likely to assist the Organisation in carrying out its function of

Schedule 1 International production orders

Part 4 International production orders relating to national security

Division 2 International production orders relating to interception: national security

Clause 89

- obtaining intelligence relating to security (so far as carrying out that function relates to the target); and
- (iii) how much the use of such methods would be likely to prejudice the Organisation in carrying out its function of obtaining intelligence relating to security (so far as carrying out that function relates to the target), whether because of delay or for any other reason; and
- (iv) such other matters (if any) as the nominated AAT Security Division member considers relevant.

Note: For *target*, see subclause (8).

Restriction on issuing order

- (6) The nominated AAT Security Division member must not issue an international production order under subclause (2) in a case where subparagraph (2)(e)(ii) applies unless the nominated AAT Security Division member is satisfied that:
 - (a) the Organisation has exhausted all other practicable methods of identifying the individual transmission services used, or likely to be used, by the other person mentioned in subparagraph (2)(e)(ii); or
 - (b) interception of communications carried by individual transmission services used or likely to be used by that other person would not otherwise be possible.
- (7) The nominated AAT Security Division member must not issue an international production order under subclause (2) in a case where subparagraph (2)(f)(ii) applies unless the nominated AAT Security Division member is satisfied that:
 - (a) the Organisation has exhausted all other practicable methods of identifying the individual message/call application services used, or likely to be used, by the other person mentioned in subparagraph (2)(f)(ii); or
 - (b) interception of messages sent or received, voice calls made or received, or video calls made or received, using individual message/call application services used or likely to be used by that other person would not otherwise be possible.

Target

- (8) For the purposes of this clause, **target** means:
- (a) if subparagraph (2)(e)(i) or (f)(i) applies—the person referred to in that subparagraph; or
 - (b) if subparagraph (2)(e)(ii) or (f)(ii) applies—the other person referred to in that subparagraph; or
 - (c) if subparagraph (2)(e)(iii) or (f)(iii) applies—the purposes referred to in that subparagraph.

90 Content of international production order

Scope

- (1) This clause applies to an international production order issued under clause 89.

Content

- (2) The order must be signed by the nominated AAT Security Division member who issued it.
- (3) The order must set out the following:
- (a) the date on which the order was issued;
 - (b) the name of the prescribed communications provider to whom the order is directed;
 - (c) the name of the designated international agreement nominated in the application for the order;
 - (d) the applicable telecommunications identifiers:
 - (i) in the case of an order that is in respect of one or more individual transmission services—to which those individual transmission services relate; or
 - (ii) in the case of an order that is in respect of one or more individual message/call application services—to which those individual message/call application services relate.
- (4) If the order directs a prescribed communications provider to intercept communications, the order may require the provider to:

Schedule 1 International production orders

Part 4 International production orders relating to national security

Division 2 International production orders relating to interception: national security

Clause 90

- (a) intercept those communications in a specified way; and
 - (b) make those intercepted communications available to the Organisation in a specified way.
- (5) A requirement under subclause (4) may:
 - (a) require that intercepted communications be made available to the Organisation directly; or
 - (b) require that intercepted communications be made available to the Organisation indirectly via the Australian Designated Authority.
- (6) If the order directs a prescribed communications provider to intercept messages, voice calls or video calls, the order may require the provider to:
 - (a) intercept those messages, voice calls or video calls in a specified way; and
 - (b) make those intercepted messages, voice calls or video calls available to the Organisation in a specified way.
- (7) A requirement under subclause (6) may:
 - (a) require that intercepted messages, voice calls or video calls be made available to the Organisation directly; or
 - (b) require that intercepted messages, voice calls or video calls be made available to the Organisation indirectly via the Australian Designated Authority.
- (8) If the order directs a prescribed communications provider to disclose telecommunications data to the Organisation, the order may require the provider to disclose that data to the Organisation in a specified way.
- (9) A requirement under subclause (8) may:
 - (a) require that the telecommunications data be disclosed to the Organisation directly; or
 - (b) require that the telecommunications data be disclosed to the Organisation indirectly via the Australian Designated Authority.

- (10) For the purposes of this clause, a specified way may deal with matters of timing.

Example: A requirement under subclause (4) may require that an intercepted communication be made available to the Organisation within 30 minutes after the communication was completed.

91 Issue of further international production order

- (1) If:

- (a) an international production order (the *original order*) was issued under clause 89; and
- (b) the original order was in respect of one or more individual transmission services; and
- (c) the original order was directed to a prescribed communications provider;

this Schedule does not prevent the issue of a further international production order under clause 89 that is:

- (d) in respect of any or all of those services; and
- (e) directed to the provider;

so long as the period specified in the further order for the purposes of subparagraph 89(2)(i)(i) of this Schedule begins after the end of the period specified in the original order for the purposes of that subparagraph.

- (2) If:

- (a) an international production order (the *original order*) was issued under clause 89; and
- (b) the original order was in respect of one or more individual message/call application services; and
- (c) the original order was directed to a prescribed communications provider;

this Schedule does not prevent the issue of a further international production order under clause 89 that is:

- (d) in respect of any or all of those services; and
- (e) directed to the provider;

Schedule 1 International production orders

Part 4 International production orders relating to national security

Division 2 International production orders relating to interception: national security

Clause 91

so long as the period specified in the further order for the purposes of subparagraph 89(2)(j)(i) of this Schedule begins after the end of the period specified in the original order for the purposes of that subparagraph.

Division 3—International production orders relating to stored communications: national security

Subdivision A—Applications

92 Application for international production order—national security

- (1) The Organisation may apply to a nominated AAT Security Division member for an international production order under clause 98 that:
 - (a) is in respect of a particular person; and
 - (b) is directed to a prescribed communications provider.
- (2) The application must nominate a designated international agreement.
- (3) The application must be made on the Organisation's behalf by:
 - (a) the Director-General of Security; or
 - (b) a Deputy Director-General of Security; or
 - (c) a senior position-holder in relation to whom an authorisation is in force under subclause (4).
- (4) The Director-General of Security may authorise in writing, for the purposes of subclause (3), senior position-holders who, or classes of senior position-holders who, are entitled under subclause (1) to make applications on the Organisation's behalf.

Attorney-General's consent to the making of an application

- (5) The Organisation must not make an application under subclause (1) unless the Attorney-General has consented to the making of the application.
- (6) The Attorney-General must not consent to the making of an application under subclause (1) for an international production

Schedule 1 International production orders

Part 4 International production orders relating to national security

Division 3 International production orders relating to stored communications: national security

Clause 92

order that is in respect of a particular person unless the Attorney-General is satisfied that:

- (a) there are reasonable grounds for suspecting that the person is engaged in, or is likely to engage in, activities prejudicial to security; and
- (b) information that would be likely to be obtained by making a copy, under an international production order issued in response to the application, of the stored communications covered by the application would be likely to assist the Organisation in carrying out its function of obtaining intelligence relating to security.

Form of Attorney-General's consent to the making of an application

- (7) Subject to subclause (8), a consent given by the Attorney-General under subclause (5) must be in writing.
- (8) If the person who proposes to make an application under subclause (1) on the Organisation's behalf thinks it necessary, because of urgent circumstances, for the Attorney-General to consent orally to the making of the application:
 - (a) the person may request the Attorney-General to consent orally to the making of the application; and
 - (b) if the person makes such a request—the Attorney-General may consent orally to the making of the application.

Note: See also clause 17A (urgent circumstances).

- (8A) At the same time as a request is made by a person under subclause (8), the person must inform the Attorney-General of the particulars of the urgent circumstances because of which the person thought it necessary for the Attorney-General to consent orally to the making of the application concerned.
 - (9) If, in response to a request made by a person under subclause (8), the Attorney-General consents orally to the making of an application, the person must:
 - (a) give the Attorney-General a written report that sets out:
-

- (i) particulars of the urgent circumstances because of which the person thought it necessary for the Attorney-General to consent orally; and
 - (ii) whether the application was granted, withdrawn or refused; and
- (b) do so within 3 working days after the day on which the application was granted, withdrawn or refused.
- (10) If, in response to a request made by a person under subclause (8), the Attorney-General consents orally to the making of an application, the Organisation must:
- (a) give the Inspector-General of Intelligence and Security a copy of the relevant report under subclause (9); and
 - (b) do so within 3 working days after the day on which the application was granted, withdrawn or refused.

93 Form of application

- (1) An application under clause 92 must be in writing.
- (2) If the person making an application under clause 92 for an international production order on the Organisation's behalf thinks it necessary, because of urgent circumstances, to make the application by telephone, the person may make the application by telephone.

Note: See also clause 17A (urgent circumstances) and clause 172 (action required).

94 Contents of written application

An application under clause 92 must, if it is in writing, set out:

- (a) a statement to the effect that the application is made by the Organisation; and
- (b) the name of the person making the application on the Organisation's behalf.

Schedule 1 International production orders

Part 4 International production orders relating to national security

Division 3 International production orders relating to stored communications: national security

Clause 95

95 Affidavits to accompany written application

- (1) An application under clause 92 must, if it is in writing, be accompanied by an affidavit complying with this clause.
- (2) The affidavit must set out the facts and other grounds on which the application is based.
- (3) Despite subclause (1), a written application may be accompanied by 2 or more affidavits that together set out each matter that, apart from this subclause, this clause would have required an affidavit accompanying the application to set out.

96 Information to be given on telephone application

The information given to a nominated AAT Security Division member in connection with a telephone application under clause 92 to the nominated AAT Security Division member:

- (a) must include particulars of the urgent circumstances because of which the person making the application on the Organisation's behalf thinks it necessary to make the application by telephone; and
- (b) must include each matter that, if the application had been made in writing, clause 94 or 95 would have required the application, or an affidavit accompanying it, to set out; and
- (c) must be given orally or in writing, as the nominated AAT Security Division member directs.

97 Giving further information to nominated AAT Security Division member

- (1) A nominated AAT Security Division member may require further information to be given in connection with an application under clause 92 to the nominated AAT Security Division member for an international production order.
- (2) The further information:

- (a) must be given on oath if the application was made in writing; and
- (b) must be given orally or otherwise, as the nominated AAT Security Division member directs.

Subdivision B—International production orders relating to stored communications

98 Issue of international production order—national security

Scope

- (1) This clause applies if the Organisation applies, under clause 92, to a nominated AAT Security Division member for an international production order that:
 - (a) is in respect of a particular person (the *relevant person*); and
 - (b) is directed to a prescribed communications provider.

Issue of international production order

- (2) If the nominated AAT Security Division member is satisfied, on the basis of the information given to the nominated AAT Security Division member under this Division in connection with the application, that:
 - (a) there are reasonable grounds for suspecting that the relevant person is engaged in, or is likely to engage in, activities prejudicial to security; and
 - (b) there are reasonable grounds for suspecting that the prescribed communications provider holds any of the following stored communications:
 - (i) stored communications that consist of communications that the relevant person has made using a telecommunications network owned or operated by the prescribed communications provider;
 - (ii) stored communications that consist of communications that another person has made using a telecommunications network owned or operated by the

Schedule 1 International production orders

Part 4 International production orders relating to national security

Division 3 International production orders relating to stored communications: national security

Clause 98

- prescribed communications provider, and for which the relevant person is the intended recipient;
- (iii) stored communications that consist of communications that the relevant person has made using a transmission service supplied by the prescribed communications provider;
 - (iv) stored communications that consist of communications that another person has made using a transmission service supplied by the prescribed communications provider, and for which the relevant person is the intended recipient;
 - (v) stored communications that consist of messages that the relevant person has sent or received using a message/call application service provided by the prescribed communications provider;
 - (vi) stored communications that consist of recordings of voice calls that the relevant person has made or received using a message/call application service provided by the prescribed communications provider;
 - (vii) stored communications that consist of recordings of video calls that the relevant person has made or received using a message/call application service provided by the prescribed communications provider;
 - (viii) stored communications that consist of material that the relevant person has uploaded for storage or back-up by a storage/back-up service provided by the prescribed communications provider;
 - (ix) stored communications that consist of material that the relevant person has posted to a general electronic content service provided by the prescribed communications provider; and
- (ba) the person who made the application on behalf of the Organisation reasonably suspects that the prescribed communications provider is based in, or operates in, a foreign country that is a party to the designated international agreement nominated in the application; and

- (c) Subdivision A has been complied with in relation to the application; and
- (d) in the case of a telephone application—because of urgent circumstances, it was necessary to make the application by telephone; and
- (e) information that would be likely to be obtained by making a copy, under an order issued under this clause, of the stored communications would be likely to assist the Organisation in carrying out its function of obtaining intelligence relating to security;

the nominated AAT Security Division member may issue an order (to be known as an *international production order*) directing the prescribed communications provider to:

- (f) make a copy of any such stored communications; and
- (g) make the copy available to the Organisation; and
- (h) if the stored communications consist of communications carried by an individual transmission service—disclose to the Organisation:
 - (i) specified telecommunications data that relates to those communications; and
 - (ii) specified telecommunications data that relates to the individual transmission service; and
- (i) if the stored communications consist of messages sent or received using an individual message/call application service—disclose to the Organisation:
 - (i) specified telecommunications data that relates to those messages; and
 - (ii) specified telecommunications data that relates to the individual message/call application service; and
- (j) if the stored communications consist of recordings of voice calls made or received using an individual message/call application service—disclose to the Organisation:
 - (i) specified telecommunications data that relates to those voice calls; and
 - (ii) specified telecommunications data that relates to the individual message/call application service; and

Schedule 1 International production orders

Part 4 International production orders relating to national security

Division 3 International production orders relating to stored communications: national security

Clause 98

- (k) if the stored communications consist of recordings of video calls made or received using an individual message/call application service—disclose to the Organisation:
 - (i) specified telecommunications data that relates to those video calls; and
 - (ii) specified telecommunications data that relates to the individual message/call application service; and
- (l) if the stored communications consist of material that has been uploaded by an end-user for storage or back-up by a storage/back-up service—disclose to the Organisation:
 - (i) specified telecommunications data that relates to that material; and
 - (ii) specified telecommunications data that relates to the end-user’s account with the storage/back-up service; and
- (m) if the stored communications consist of material posted to a general electronic content service by an end-user—disclose to the Organisation:
 - (i) specified telecommunications data that relates to that material; and
 - (ii) specified telecommunications data that relates to the end-user’s account with the general electronic content service.

Matters to which nominated AAT Security Division member must have regard

- (3) In deciding whether to issue an international production order under subclause (2), the nominated AAT Security Division member must have regard to the following matters:
 - (a) to what extent methods of carrying out the Organisation’s function of obtaining intelligence relating to security (so far as carrying out that function relates to the relevant person) that are less intrusive than obtaining, under such an order, a copy of the stored communications have been used by, or are available to, the Organisation;

- (b) how much the use of such methods would be likely to assist the Organisation in carrying out its function of obtaining intelligence relating to security (so far as carrying out that function relates to the relevant person);
- (c) how much the use of such methods would be likely to prejudice the Organisation in carrying out its function of obtaining intelligence relating to security (so far as carrying out that function relates to the relevant person);
- (d) such other matters (if any) as the nominated AAT Security Division member considers relevant.

99 Content of international production order

Scope

- (1) This clause applies to an international production order issued under clause 98.

Content

- (2) The order must be signed by the nominated AAT Security Division member who issued it.
- (3) The order must set out the following:
 - (a) the date on which the order was issued;
 - (b) the name of the prescribed communications provider to whom the order is directed;
 - (c) the name of the designated international agreement nominated in the application for the order.
- (4) If the order directs a prescribed communications provider to make a copy of stored communications available to the Organisation, the order may require the provider to make that copy available to the Organisation in a specified way.
- (5) A requirement under subclause (4) may:
 - (a) require that a copy of stored communications be made available to the Organisation directly; or

Schedule 1 International production orders

Part 4 International production orders relating to national security

Division 3 International production orders relating to stored communications: national security

Clause 100

- (b) require that a copy of stored communications be made available to the Organisation indirectly via the Australian Designated Authority.
- (6) If the order directs a prescribed communications provider to disclose telecommunications data to the Organisation, the order may require the provider to disclose that data to the Organisation in a specified way.
- (7) A requirement under subclause (6) may:
 - (a) require that the telecommunications data be disclosed to the Organisation directly; or
 - (b) require that the telecommunications data be disclosed to the Organisation indirectly via the Australian Designated Authority.
- (8) For the purposes of this clause, a specified way may deal with matters of timing.

100 Issue of further international production order

If:

- (a) an international production order (the *original order*) was issued under clause 98; and
- (b) the original order was in respect of a particular person; and
- (c) the original order was directed to a prescribed communications provider;

this Schedule does not prevent the issue of a further international production order under clause 98 that:

- (d) is in respect of the person; and
- (e) is directed to the provider.

Division 4—International production orders relating to telecommunications data: national security

Subdivision A—Applications

101 Application for international production order—national security

- (1) The Organisation may apply to a nominated AAT Security Division member for an international production order under clause 107 that:
 - (a) is in respect of a particular person; and
 - (b) is directed to a prescribed communications provider.
- (2) The application must nominate a designated international agreement.
- (3) The application must be made on the Organisation's behalf by:
 - (a) the Director-General of Security; or
 - (b) a Deputy Director-General of Security; or
 - (c) an eligible position-holder in relation to whom an authorisation is in force under subclause (4).
- (4) The Director-General of Security may authorise in writing, for the purposes of subclause (3), eligible position-holders who, or classes of eligible position-holders who, are entitled under subclause (1) to make applications on the Organisation's behalf.

102 Form of application

- (1) An application under clause 101 must be in writing.
- (2) If the person making an application under clause 101 for an international production order on the Organisation's behalf thinks it necessary, because of urgent circumstances, to make the application by telephone, the person may make the application by telephone.

Schedule 1 International production orders

Part 4 International production orders relating to national security

Division 4 International production orders relating to telecommunications data:
national security

Clause 103

Note: See also clause 17A (urgent circumstances) and clause 172 (action required).

103 Contents of written application

An application under clause 101 must, if it is in writing, set out:

- (a) a statement to the effect that the application is made by the Organisation; and
- (b) the name of the person making the application on the Organisation's behalf.

104 Affidavits to accompany written application

- (1) An application under clause 101 must, if it is in writing, be accompanied by an affidavit complying with this clause.
- (2) The affidavit must set out the facts and other grounds on which the application is based.
- (3) Despite subclause (1), a written application may be accompanied by 2 or more affidavits that together set out each matter that, apart from this subclause, this clause would have required an affidavit accompanying the application to set out.

105 Information to be given on telephone application

The information given to a nominated AAT Security Division member in connection with a telephone application under clause 101 to the nominated AAT Security Division member:

- (a) must include particulars of the urgent circumstances because of which the person making the application on the Organisation's behalf thinks it necessary to make the application by telephone; and
- (b) must include each matter that, if the application had been made in writing, clause 103 or 104 would have required the application, or an affidavit accompanying it, to set out; and
- (c) must be given orally or in writing, as the nominated AAT Security Division member directs.

106 Giving further information to nominated AAT Security Division member

- (1) A nominated AAT Security Division member may require further information to be given in connection with an application under clause 101 to the nominated AAT Security Division member for an international production order.
- (2) The further information:
 - (a) must be given on oath if the application was made in writing; and
 - (b) must be given orally or otherwise, as the nominated AAT Security Division member directs.

Subdivision B—International production orders relating to telecommunications data

107 Issue of international production order—national security

Scope

- (1) This clause applies if the Organisation applies, under clause 101, to a nominated AAT Security Division member for an international production order that:
 - (a) is in respect of a particular person (the *relevant person*); and
 - (b) is directed to a prescribed communications provider.

Issue of international production order

- (2) If the nominated AAT Security Division member is satisfied, on the basis of the information given to the nominated AAT Security Division member under this Division in connection with the application, that:
 - (a) there are reasonable grounds for suspecting that the prescribed communications provider holds, or is likely to commence to hold, any of the following telecommunications data:

Schedule 1 International production orders

Part 4 International production orders relating to national security

Division 4 International production orders relating to telecommunications data:
national security

Clause 107

- (i) telecommunications data that relates to communications that the relevant person has made using an individual transmission service supplied by the prescribed communications provider;
- (ii) telecommunications data that relates to an individual transmission service supplied using a telecommunications network owned or operated by the prescribed communications provider, where the individual transmission service is used, or is likely to be used, by the relevant person;
- (iii) telecommunications data that relates to an individual transmission service supplied by the prescribed communications provider, where the individual transmission service is used, or is likely to be used, by the relevant person;
- (iv) telecommunications data that relates to messages sent or received by the relevant person using an individual message/call application service provided by the prescribed communications provider;
- (v) telecommunications data that relates to voice calls made or received by the relevant person using an individual message/call application service provided by the prescribed communications provider;
- (vi) telecommunications data that relates to video calls made or received by the relevant person using an individual message/call application service provided by the prescribed communications provider;
- (vii) telecommunications data that relates to an individual message/call application service provided by the prescribed communications provider, where the individual message/call application service is used, or is likely to be used, by the relevant person;
- (viii) telecommunications data that relates to material that has been uploaded by the relevant person for storage or back-up by a storage/back-up service provided by the prescribed communications provider;

- (ix) telecommunications data that relates to material that has been posted by the relevant person on a general electronic content service provided by the prescribed communications provider; and
- (aa) the person who made the application on behalf of the Organisation reasonably suspects that the prescribed communications provider is based in, or operates in, a foreign country that is a party to the designated international agreement nominated in the application; and
- (b) Subdivision A has been complied with in relation to the application; and
- (c) in the case of a telephone application—because of urgent circumstances, it was necessary to make the application by telephone; and
- (d) disclosing the telecommunications data to the Organisation, under an order issued under this clause, would be in connection with the performance by the Organisation of its functions;

the nominated AAT Security Division member may issue an order (to be known as an *international production order*) directing the prescribed communications provider to do either or both of the following:

- (e) so far as the telecommunications data is held by the prescribed communications provider when the international production order comes into force—disclose any such telecommunications data to the Organisation;
- (f) so far as the telecommunications data commences to be held by the prescribed communications provider during a specified period—disclose any such telecommunications data to the Organisation.

Period specified in international production order

- (3) A period specified in an international production order for the purposes of paragraph (2)(f) must not begin before the time when the order is given to the prescribed communications provider.

Note: International production orders are given under clause 112.

Schedule 1 International production orders

Part 4 International production orders relating to national security

Division 4 International production orders relating to telecommunications data:
national security

Clause 108

- (4) A period specified in an international production order for the purposes of paragraph (2)(f) must not be longer than 90 days.

Matters to which nominated AAT Security Division member must have regard

- (5) In deciding whether to issue an international production order under subclause (2), the nominated AAT Security Division member must have regard to the following matters:
- (a) to what extent methods of performing the Organisation's functions (so far as performing those functions relates to the relevant person) that are less intrusive than obtaining, under such an order, the telecommunications data have been used by, or are available to, the Organisation;
 - (b) how much the use of such methods would be likely to assist the Organisation in performing its functions (so far as performing those functions relates to the relevant person);
 - (c) how much the use of such methods would be likely to prejudice the Organisation in performing its functions (so far as performing those functions relates to the relevant person), whether because of delay or for any other reason;
 - (d) such other matters (if any) as the nominated AAT Security Division member considers relevant.

108 Content of international production order

Scope

- (1) This clause applies to an international production order issued under clause 107.

Content

- (2) The order must be signed by the nominated AAT Security Division member who issued it.
- (3) The order must set out the following:
- (a) the date on which the order was issued;

- (b) the name of the prescribed communications provider to whom the order is directed;
 - (c) the name of the designated international agreement nominated in the application for the order.
- (4) If the order directs a prescribed communications provider to disclose telecommunications data to the Organisation, the order may require the provider to disclose that data to the Organisation in a specified way.
- (5) A requirement under subclause (4) may:
- (a) require that the telecommunications data be disclosed to the Organisation directly; or
 - (b) require that the telecommunications data be disclosed to the Organisation indirectly via the Australian Designated Authority.
- (6) For the purposes of this clause, a specified way may deal with matters of timing.

Example: If a requirement under subclause (4) relates to telecommunications data that commences to be held by a prescribed communications provider during a specified period, the requirement may require that the telecommunications data be disclosed to the Organisation within 30 minutes after the telecommunications data commences to be held.

109 Issue of further international production order

If:

- (a) an international production order (the *original order*) was issued under clause 107; and
- (b) the original order was in respect of a particular person; and
- (c) the original order was directed to a prescribed communications provider;

this Schedule does not prevent the issue of a further international production order under clause 107 that:

- (d) is in respect of the person; and
- (e) is directed to the provider.

Part 5—Giving of international production orders

110 Simplified outline of this Part

- Before an international production order is given to a prescribed communications provider, the Australian Designated Authority must consider whether the order complies with the designated international agreement nominated in the application for the order.
- If the Australian Designated Authority is satisfied that the order complies with the designated international agreement nominated in the application for the order, the Australian Designated Authority must give the order to the prescribed communications provider. The order comes in force when it is given to the provider.
- If the Australian Designated Authority is not satisfied that the order complies with the designated international agreement nominated in the application for the order, the Australian Designated Authority must cancel the order.

111 Giving of international production orders—relevant agency

- (1) If an international production order is issued under Part 2 or 3 of this Schedule:
 - (a) the relevant agency that applied for the order must:
 - (i) give the order, or a certified copy of the order, to the Australian Designated Authority; and
 - (ii) do so as soon as practicable after the order is issued; and
 - (b) the Australian Designated Authority must consider whether the order complies with the designated international agreement nominated in the application for the order; and

- (c) if the Australian Designated Authority is satisfied that the order complies with the designated international agreement nominated in the application for the order—the Australian Designated Authority must:
 - (i) give the order, or the certified copy of the order, to the prescribed communications provider to whom the order is directed; and
 - (ii) do so as soon as practicable after becoming so satisfied; and
- (d) if the Australian Designated Authority is not satisfied that the order complies with the designated international agreement nominated in the application for the order—the Australian Designated Authority must:
 - (i) cancel the order; and
 - (ii) return the order, or the certified copy of the order, to the agency; and
 - (iii) give the agency such advice as the Australian Designated Authority considers appropriate in relation to compliance with the designated international agreement.

Note: See clause 171 (which deals with electronic service of documents).

- (2) For the purposes of this Schedule, if the Australian Designated Authority gives a certified copy of an international production order to a prescribed communications provider under subclause (1), the Australian Designated Authority is taken to have given the order to the prescribed communications provider under subclause (1).
- (3) An international production order issued under Part 2 or 3 of this Schedule comes into force when it is given to the prescribed communications provider to whom the order is directed.
- (4) For the purposes of this Schedule, if the Australian Designated Authority gives an international production order to a prescribed communications provider under subclause (1), the order is taken to invoke the designated international agreement nominated in the application for the order.

Clause 112

- (5) If the Australian Designated Authority gives an international production order to a prescribed communications provider under subclause (1), the Australian Designated Authority must notify the giving of the order to the relevant agency that applied for the order.
- (6) A cancellation under paragraph (1)(d) is to be set out in a written instrument.
- (7) If an international production order is issued under Part 2 or 3 of this Schedule, the relevant agency that applied for the order may give the Australian Designated Authority information that is likely to assist the Australian Designated Authority in making a decision under this clause in relation to the order.

112 Giving of international production orders—the Organisation

- (1) If an international production order is issued under Part 4 of this Schedule:
 - (a) the Organisation must:
 - (i) give the order, or a certified copy of the order, to the Australian Designated Authority; and
 - (ii) do so as soon as practicable after the order is issued; and
 - (b) the Australian Designated Authority must consider whether the order complies with the designated international agreement nominated in the application for the order; and
 - (c) if the Australian Designated Authority is satisfied that the order complies with the designated international agreement nominated in the application for the order—the Australian Designated Authority must:
 - (i) give the order, or the certified copy of the order, to the prescribed communications provider to whom the order is directed; and
 - (ii) do so as soon as practicable after becoming so satisfied; and
 - (d) if the Australian Designated Authority is not satisfied that the order complies with the designated international agreement

nominated in the application for the order—the Australian Designated Authority must:

- (i) cancel the order; and
- (ii) return the order, or the certified copy of the order, to the Organisation; and
- (iii) give the Organisation such advice as the Australian Designated Authority considers appropriate in relation to compliance with the designated international agreement.

Note: See clause 171 (which deals with electronic service of documents).

- (2) For the purposes of this Schedule, if the Australian Designated Authority gives a certified copy of an international production order to a prescribed communications provider under subclause (1), the Australian Designated Authority is taken to have given the order to the prescribed communications provider under subclause (1).
- (3) An international production order issued under Part 4 of this Schedule comes into force when it is given to the prescribed communications provider to whom the order is directed.
- (4) For the purposes of this Schedule, if the Australian Designated Authority gives an international production order to a prescribed communications provider under subclause (1), the order is taken to invoke the designated international agreement nominated in the application for the order.
- (5) If the Australian Designated Authority gives an international production order to a prescribed communications provider under subclause (1), the Australian Designated Authority must notify the giving of the order to the Organisation.
- (6) A cancellation under paragraph (1)(d) is to be set out in a written instrument.
- (7) If an international production order is issued under Part 4 of this Schedule, the Organisation may give the Australian Designated Authority information that is likely to assist the Australian

Schedule 1 International production orders
Part 5 Giving of international production orders

Clause 112

Designated Authority in making a decision under this clause in relation to the order.

Part 6—Revocation of international production orders

113 Simplified outline of this Part

- If an international production order was issued in response to an application made by a relevant agency, the chief officer of the agency:
 - (a) may revoke the order; and
 - (b) must revoke the order if the chief officer is satisfied that the grounds on which the order was issued have ceased to exist.
- If an international production order was issued in response to an application made by the Organisation, the Director-General of Security:
 - (a) may revoke the order; and
 - (b) must revoke the order if the Director-General of Security is satisfied that the grounds on which the order was issued have ceased to exist.
- If an international production order is revoked after it has come into force, the Australian Designated Authority must give the instrument of revocation to the prescribed communications provider to whom the order is directed.

114 Revocation of international production orders—relevant agency

- (1) If:
- (a) an international production order was issued under Part 2 or 3 of this Schedule; and
 - (b) the order was issued in response to an application made by a relevant agency;

Clause 115

the chief officer of the agency:

- (c) may revoke the order; and
 - (d) must revoke the order if the chief officer is satisfied that the grounds on which the order was issued have ceased to exist.
- (2) A revocation under this clause is to be set out in a written instrument.
- (3) For the purposes of the application of subclause (1) to an international production order issued under Part 3 of this Schedule on the ground that a Part 5.3 supervisory order was in force in relation to a particular person when the international production order was issued, that ground is taken to have ceased to exist if, and only if, neither that Part 5.3 supervisory order, nor any succeeding Part 5.3 supervisory order, is in force.

115 Giving of instrument of revocation—relevant agency

- (1) If an international production order is revoked under clause 114 by the chief officer of a relevant agency, the relevant agency must:
- (a) give the instrument of revocation to the Australian Designated Authority; and
 - (b) do so as soon as practicable after the order is revoked.
- (2) If:
- (a) the Australian Designated Authority gave an international production order to the prescribed communications provider to whom the order is directed; and
 - (b) the order was subsequently revoked under clause 114;
- the Australian Designated Authority must:
- (c) give the instrument of revocation to the prescribed communications provider; and
 - (d) do so as soon as practicable after the instrument of revocation is given to the Australian Designated Authority.
- (3) A revocation under clause 114 takes effect:

- (a) if the instrument of revocation is required to be given to the prescribed communications provider concerned—when the instrument is given; or
 - (b) otherwise—when the revocation is made.
- (4) If:
- (a) an international production order is revoked under clause 114; and
 - (b) when the revocation takes effect, the Australian Designated Authority has not made a decision about the order under clause 111;
- clause 111 ceases to apply to the order when the revocation takes effect.

116 Revocation of international production orders—the Organisation

- (1) If an international production order was issued under Part 4 of this Schedule, the Director-General of Security:
 - (a) may revoke the order; and
 - (b) must revoke the order if the Director-General of Security is satisfied that the grounds on which the order was issued have ceased to exist.
- (2) A revocation under this clause is to be set out in a written instrument.

117 Giving of instrument of revocation—the Organisation

- (1) If an international production order is revoked under clause 116 by the Director-General of Security, the Organisation must:
 - (a) give the instrument of revocation to the Australian Designated Authority; and
 - (b) do so as soon as practicable after the order is revoked.

Clause 118

- (2) If:
- (a) the Australian Designated Authority gave an international production order to the prescribed communications provider to whom the order is directed; and
 - (b) the order was subsequently revoked under clause 116;
- the Australian Designated Authority must:
- (c) give the instrument of revocation to the prescribed communications provider; and
 - (d) do so as soon as practicable after the instrument of revocation is given to the Australian Designated Authority.
- (3) A revocation under clause 116 takes effect:
- (a) if the instrument of revocation is required to be given to the prescribed communications provider concerned—when the instrument is given; or
 - (b) otherwise—when the revocation is made.
- (4) If:
- (a) an international production order is revoked under clause 116; and
 - (b) when the revocation takes effect, the Australian Designated Authority has not made a decision about the order under clause 112;
- clause 112 ceases to apply to the order when the revocation takes effect.

118 Delegation by the chief officer of a relevant agency

- (1) The chief officer of a relevant agency may, by writing, delegate any or all of the chief officer's functions or powers under this Part to a certifying officer of the agency.
- (2) In performing functions, or exercising powers, under a delegation under subclause (1), the delegate must comply with any directions of the chief officer.

119 Delegation by the Director-General of Security

- (1) The Director-General of Security may, by writing, delegate any or all of the Director-General of Security's functions or powers under this Part to a person who is:
 - (a) a Deputy Director-General of Security; or
 - (b) an ASIO employee.
- (2) In performing functions, or exercising powers, under a delegation under subclause (1), the delegate must comply with any directions of the Director-General of Security.

Part 7—Objections to, and cancellation of, international production orders

120 Simplified outline of this Part

- If an international production order is given to a prescribed communications provider, the provider may object to the order on the grounds that the order does not comply with the designated international agreement nominated in the application for the order.
- The Australian Designated Authority may cancel an international production order.

121 Prescribed communications provider may object to international production order

- (1) If an international production order is given to the prescribed communications provider to whom the order is directed, the provider may, by written notice given to the Australian Designated Authority, object to the order on the grounds that the order does not comply with the designated international agreement nominated in the application for the order.
- (2) The notice must:
 - (a) be given to the Australian Designated Authority within a reasonable time after the international production order is given to the prescribed communications provider; and
 - (b) set out the reasons why the provider considers that the order does not comply with the designated international agreement nominated in the application for the order.

122 Cancellation of international production orders

- (1) The Australian Designated Authority may cancel an international production order.
- (2) A cancellation under subclause (1) is to be set out in a written instrument.
- (3) If an international production order is cancelled under subclause (1), the Australian Designated Authority must:
 - (a) if the order was issued under Part 2 or 3 of this Schedule in response to an application by a relevant agency:
 - (i) inform the chief officer of the relevant agency of the cancellation; and
 - (ii) do so as soon as practicable after cancelling the order; or
 - (b) if the order was issued under Part 4 of this Schedule:
 - (i) inform the Organisation of the cancellation; and
 - (ii) do so as soon as practicable after cancelling the order.
- (4) If:
 - (a) the Australian Designated Authority gave an international production order to the prescribed communications provider to whom the order is directed; and
 - (b) the order was subsequently cancelled under subclause (1);the Australian Designated Authority must:
 - (c) give the instrument of cancellation to the prescribed communications provider; and
 - (d) do so as soon as practicable after cancelling the order.
- (5) A cancellation under subclause (1) takes effect:
 - (a) if the instrument of cancellation is required to be given to the prescribed communications provider concerned—when the instrument is given; or
 - (b) otherwise—when the cancellation is made.
- (6) If:

Schedule 1 International production orders

Part 7 Objections to, and cancellation of, international production orders

Clause 122

- (a) an international production order is cancelled under this clause; and
 - (b) when the cancellation takes effect, the Australian Designated Authority has not made a decision about the order under clause 111 or 112 (as the case may be);
- clause 111 or 112 (as the case may be) ceases to apply to the order when the cancellation takes effect.

Part 8—Compliance with international production orders

123 Simplified outline of this Part

- Civil penalties apply for failing to comply with international production orders.

124 Compliance with international production orders

If:

- (a) an international production order is given to the prescribed communications provider to whom the order is directed; and
- (b) the order is in force; and
- (c) when the order is given, the prescribed communications provider meets the enforcement threshold;

the prescribed communications provider must comply with the order to the extent to which the prescribed communications provider is capable of doing so.

Civil penalty: 238 penalty units.

125 When a prescribed communications provider meets the enforcement threshold

- (1) For the purposes of this Schedule, if:
 - (a) a prescribed communications provider owns or operates a telecommunications network that is used to supply a transmission service to one or more Australians; or
 - (b) a prescribed communications provider supplies a transmission service to one or more Australians; or
 - (c) a prescribed communications provider provides a message/call application service to one or more Australians;or

Clause 125

- (d) a prescribed communications provider provides a storage/back-up service to one or more Australians; or
- (e) one or more Australians have posted material on a general electronic content service provided by a prescribed communications provider;

the prescribed communications provider *meets the enforcement threshold* unless:

- (f) if paragraph (a) applies—the provider of a transmission service supplied using the telecommunications network cannot reasonably be considered to have offered or provided the transmission service on the basis of the service being available to Australians; and
- (g) if paragraph (b) applies—the prescribed communications provider cannot reasonably be considered to have offered or provided the transmission service on the basis of the service being available to Australians; and
- (h) if paragraph (c) applies—the prescribed communications provider cannot reasonably be considered to have offered or provided the message/call application service on the basis of the service being available to Australians; and
- (i) if paragraph (d) applies—the prescribed communications provider cannot reasonably be considered to have offered or provided the storage/back-up service on the basis of the service being available to Australians; and
- (j) if paragraph (e) applies—the prescribed communications provider cannot reasonably be considered to have offered or provided the general electronic content service on the basis of the opportunity to post material on the service being available to Australians.

Australian

- (2) For the purposes of this clause, *Australian* means an individual who is ordinarily resident in Australia.

126 Civil penalty provision—enforcement

Enforceable civil penalty provision

- (1) A civil penalty provision in this Part is enforceable under Part 4 of the *Regulatory Powers (Standard Provisions) Act 2014*.

Note: Part 4 of the *Regulatory Powers (Standard Provisions) Act 2014* allows a civil penalty provision to be enforced by obtaining an order for a person to pay a pecuniary penalty for the contravention of the provision.

Authorised applicant

- (2) For the purposes of Part 4 of the *Regulatory Powers (Standard Provisions) Act 2014*, the Communications Access Co-ordinator is an authorised applicant in relation to a civil penalty provision in this Part.

Relevant court

- (3) For the purposes of Part 4 of the *Regulatory Powers (Standard Provisions) Act 2014*, the Federal Court of Australia and the Federal Circuit and Family Court of Australia are relevant courts in relation to a civil penalty provision in this Part.

Penalty for a body corporate

- (4) Paragraph 82(5)(a) of the *Regulatory Powers (Standard Provisions) Act 2014*, as it applies in relation to a civil penalty provision in this Part, has effect as if “5 times” were omitted and “200 times” were substituted.

Extra-territorial application

- (5) Part 4 of the *Regulatory Powers (Standard Provisions) Act 2014*, as it applies in relation to a civil penalty provision in this Part, extends to acts, omissions, matters and things outside Australia.

Part 9—Reporting and record-keeping requirements

Division 1—Introduction

127 Simplified outline of this Part

- The chief officer of a relevant agency and the Australian Designated Authority must give the Minister annual reports about matters relating to international production orders.
- The Director-General of Security must give the Attorney-General a report on the extent to which compliance by a prescribed communications provider with an international production order has assisted the Organisation in carrying out its functions.
- The Minister must cause to be prepared annual reports about matters relating to international production orders that were issued in response to applications made by relevant agencies.
- The chief officer of a relevant agency, the Director-General of Security and the Australian Designated Authority must ensure that records are kept of matters relating to international production orders.

Division 2—Reporting requirements

128 Annual reports by relevant agencies

The chief officer of a relevant agency must, within 3 months after the end of each financial year, give the Minister a written report that sets out:

- (a) the relevant statistics about applications made by the agency under clause 22 during the financial year; and
- (b) the relevant statistics about applications made by the agency under clause 33 during the financial year; and
- (c) the relevant statistics about applications made by the agency under clause 42 during the financial year; and
- (d) the relevant statistics about applications made by the agency under clause 52 during the financial year; and
- (e) the relevant statistics about applications made by the agency under clause 63 during the financial year; and
- (f) the relevant statistics about applications made by the agency under clause 72 during the financial year; and
- (g) for each designated international agreement—the number of applications made by the agency under Part 2 or 3 of this Schedule during the financial year that nominated the designated international agreement; and
- (h) if one or more international production orders were issued before the end of the financial year in response to applications made by the agency:
 - (i) the number of occasions during the financial year on which protected information obtained in accordance with those orders was shared with other relevant agencies; and
 - (ii) the number of arrests that were made during the financial year on the basis of protected information obtained in accordance with those orders; and

Clause 129

- (iii) the number of prosecutions where protected information obtained in accordance with those orders was used in evidence during the financial year; and
- (iv) the number of convictions during the financial year where protected information obtained in accordance with those orders was used in evidence in the prosecutions that resulted in those convictions; and
- (i) if one or more international production orders were issued under clause 30 during the financial year, in response to applications made by the agency, on grounds relating to the investigation of one or more offences—the type or types of those offences; and
- (j) if one or more international production orders were issued under clause 39 during the financial year, in response to applications made by the agency, on grounds relating to the investigation of one or more offences—the type or types of those offences; and
- (k) if one or more international production orders were issued under clause 48 during the financial year, in response to applications made by the agency, on grounds relating to the investigation of one or more offences—the type or types of those offences; and
- (l) the number of international production orders revoked by the chief officer under clause 114 during the financial year; and
- (m) if subparagraph 30(2)(g)(ii) or (h)(ii) applied to one or more international production orders issued under clause 30 during the financial year in response to applications made by the agency—the number of those orders; and
- (n) if subparagraph 60(2)(g)(ii) or (h)(ii) applied to one or more international production orders issued under clause 60 during the financial year in response to applications made by the agency—the number of those orders.

**129 Reports to be made to the Attorney-General by the
Director-General of Security**

The Director-General of Security must:

- (a) give the Attorney-General, in respect of each international production order issued under clause 89, a written report on the extent to which compliance by a prescribed communications provider with the order has assisted the Organisation in carrying out its functions; and
- (b) do so within 3 months after whichever of the following first occurs:
 - (i) the end of the last day on which the prescribed communications provider could have done an act or thing in compliance with the order;
 - (ii) the time when the order ceases to be in force because of the revocation or cancellation of the order.

130 Annual reports by the Australian Designated Authority

- (1) The Australian Designated Authority must, within 3 months after the end of each financial year, give the Minister a written report that sets out, for each relevant agency:
 - (a) if one or more international production orders issued in response to applications made by the agency were given by the Australian Designated Authority to prescribed communications providers during the financial year:
 - (i) the number of those orders; and
 - (ii) the number of each type of those orders; and
 - (iii) for each designated international agreement—the number of those orders that invoked the designated international agreement; and
 - (b) if subparagraph 30(2)(g)(ii) or (h)(ii) applied to one or more international production orders that were:
 - (i) issued under clause 30 in response to applications made by the agency; and
 - (ii) given by the Australian Designated Authority to prescribed communications providers during the financial year;
- the number of those orders; and

Clause 130

- (c) if subparagraph 60(2)(g)(ii) or (h)(ii) applied to one or more international production orders that were:
 - (i) issued under clause 60 in response to applications made by the agency; and
 - (ii) given by the Australian Designated Authority to prescribed communications providers during the financial year;the number of those orders; and
 - (d) if one or more international production orders issued in response to applications made by the agency were cancelled by the Australian Designated Authority under clause 111 during the financial year—the number of those orders; and
 - (e) if one or more international production orders issued in response to applications made by the agency were cancelled by the Australian Designated Authority under clause 122 during the financial year—the number of those orders; and
 - (f) if one or more instruments of revocation of international production orders issued in response to applications made by the agency were given by the Australian Designated Authority to prescribed communications providers during the financial year—the number of those instruments; and
 - (g) if one or more objections were received by the Australian Designated Authority under clause 121 during the financial year in relation to international production orders issued in response to applications made by the agency:
 - (i) the number of international production orders to which those objections relate; and
 - (ii) the number of each type of those orders; and
 - (iii) for each designated international agreement—the number of those orders that invoked the designated international agreement.
- (2) The Minister must:
- (a) cause a copy of a report under subclause (1) to be given to the Attorney-General; and
 - (b) do so as soon as practicable after receiving the report.

131 Annual reports by the Minister

- (1) The Minister must, as soon as practicable after the end of each financial year, cause to be prepared a written report that:
 - (a) sets out, for each relevant agency, the information contained in the report by the chief officer of the agency under clause 128 for the financial year; and
 - (b) sets out the information contained in the report by the Australian Designated Authority under clause 130 for the financial year.

Report to be tabled

- (2) The Minister must cause a copy of a report under subclause (1) to be tabled in each House of the Parliament within 15 sitting days of that House after the report is prepared.
- (3) A report under subclause (1) must not be made in a manner that is likely to enable the identification of a person.
- (4) For the purposes of section 34C of the *Acts Interpretation Act 1901*, a report that subclause (1) requires to be prepared as soon as practicable after the end of a financial year is taken to be a periodic report that this Act requires a person to furnish to the Minister and that relates to the administration of this Schedule during the financial year.

132 Deferral of inclusion of information in Ministerial report

Scope

- (1) This clause applies to information:
 - (a) included in a report given to the Minister:
 - (i) under clause 128 by the chief officer of a relevant agency; or
 - (ii) under clause 130 by the Australian Designated Authority; and

Clause 132

- (b) that the Minister would, apart from this clause, be required to include in the next Ministerial report.

Exclusion of information—relevant agency

- (2) If:
 - (a) subparagraph (1)(a)(i) applies; and
 - (b) the chief officer of the relevant agency is satisfied that the information is Part 5.3 information;the chief officer must advise the Minister in writing not to include the information in the next Ministerial report.
- (3) If the Minister is satisfied, on the advice of the chief officer, that the information is Part 5.3 information, the Minister must:
 - (a) notify the chief officer in writing; and
 - (b) not include the information in any Ministerial report until the Minister decides otherwise under subclause (5).

Inclusion of information in subsequent report—relevant agency

- (4) If the information has not been included in a Ministerial report because of subclause (3), the chief officer must, before the Minister prepares the next Ministerial report:
 - (a) reconsider whether the information is Part 5.3 information; and
 - (b) if the chief officer is satisfied that the information is not Part 5.3 information—advise the Minister in writing to include the information in the next Ministerial report.
- (5) If the Minister is satisfied, on the advice of the chief officer, that the information is not Part 5.3 information, the Minister must:
 - (a) notify the chief officer in writing; and
 - (b) include the information in the next Ministerial report.

Exclusion of information—Australian Designated Authority

- (6) If:
 - (a) subparagraph (1)(a)(ii) applies; and

- (b) the Australian Designated Authority is satisfied that the information is Part 5.3 information;
- the Australian Designated Authority must advise the Minister in writing not to include the information in the next Ministerial report.
- (7) If the Minister is satisfied, on the advice of the Australian Designated Authority, that the information is Part 5.3 information, the Minister must:
- (a) notify the Australian Designated Authority in writing; and
 - (b) not include the information in any Ministerial report until the Minister decides otherwise under subclause (9).

Inclusion of information in subsequent report—Australian Designated Authority

- (8) If the information has not been included in a Ministerial report because of subclause (7), the Australian Designated Authority must, before the Minister prepares the next Ministerial report:
- (a) reconsider whether the information is Part 5.3 information; and
 - (b) if the Australian Designated Authority is satisfied that the information is not Part 5.3 information—advise the Minister in writing to include the information in the next Ministerial report.
- (9) If the Minister is satisfied, on the advice of the Australian Designated Authority, that the information is not Part 5.3 information, the Minister must:
- (a) notify the chief officer in writing; and
 - (b) include the information in the next Ministerial report.

Definitions

- (10) In this clause:

Ministerial report means a report the Minister causes to be prepared under clause 131.

Clause 132

Part 5.3 information means information that, if made public, could reasonably be expected to enable a reasonable person to conclude that:

- (a) an international production order is likely to be, or is not likely to be, in force under Part 3 of this Schedule in relation to:
 - (i) an individual carriage service used, or likely to be used, by a particular person; or
 - (ii) an individual message/call application service used, or likely to be used, by a particular person; or
 - (iii) stored communications that consist of communications that a particular person has made using an individual carriage service; or
 - (iv) stored communications that consist of messages that a particular person has sent or received using an individual message/call application service; or
 - (v) stored communications that consist of recordings of voice calls that a particular person has made or received using an individual message/call application service; or
 - (vi) stored communications that consist of recordings of video calls that a particular person has made or received using an individual message/call application service; or
 - (vii) stored communications that consist of material that a particular person has uploaded for storage or back-up by a storage/back-up service; or
 - (viii) stored communications that consist of material that a particular person has posted to a general electronic content service; or
 - (ix) telecommunications data that relates to communications that a particular person has made using an individual carriage service; or
 - (x) telecommunications data that relates to an individual carriage service used, or likely to be used, by a particular person; or

- (xi) telecommunications data that relates to messages sent or received by a particular person using an individual message/call application service; or
 - (xii) telecommunications data that relates to voice calls made or received by a particular person using an individual message/call application service; or
 - (xiii) telecommunications data that relates to video calls made or received by a particular person using an individual message/call application service; or
 - (xiv) telecommunications data that relates to an individual message/call application service used, or likely to be used, by a particular person; or
 - (xv) telecommunications data that relates to material that has been uploaded by a particular person for storage or back-up by a storage/back-up service; or
 - (xvi) telecommunications data that relates to material that has been posted by a particular person on a general electronic content service; or
- (b) an international production order is likely to be, or is not likely to be, in force under Part 3 of this Schedule in relation to a particular person.

Division 3—Record-keeping requirements

133 Keeping documents associated with international production orders—relevant agencies

- (1) The chief officer of a relevant agency must cause the following to be kept in the agency's records:
 - (a) a copy of each written application made by the agency for an international production order;
 - (b) a copy of each affidavit that accompanied a written application made by the agency for an international production order;
 - (c) a copy of each international production order issued in response to an application made by the agency;
 - (d) a copy of each authorisation given by the chief officer under subclause 23(3);
 - (e) a copy of each authorisation given by the chief officer under subclause 34(3);
 - (f) a copy of each authorisation given by the chief officer under subclause 43(3);
 - (g) a copy of each authorisation given by the chief officer under subclause 53(3);
 - (h) a copy of each authorisation given by the chief officer under subclause 64(3);
 - (i) a copy of each authorisation given by the chief officer under subclause 73(3);
 - (j) if the chief officer revokes an international production order under clause 114—a copy of the instrument of revocation.
- (2) The period for which the chief officer of a relevant agency must cause a copy of a particular document to be kept in the agency's records under subclause (1) is the period:
 - (a) starting when the document came into existence; and
 - (b) ending:

- (i) when 3 years have elapsed since the document came into existence; or
 - (ii) when the Ombudsman gives a report to the Minister under clause 150 that is about records that include the copy;
- whichever happens earlier.

134 Other records to be kept—relevant agencies

- (1) The chief officer of a relevant agency must cause the following to be kept in the agency's records:
 - (a) details of each telephone application made by the agency for an international production order;
 - (b) for each application made by the agency for an international production order—a statement as to whether the application was granted, refused or withdrawn;
 - (c) for each international production order issued in response to an application made by the agency:
 - (i) a record of the type of order; and
 - (ii) a record of the designated international agreement nominated in the application; and
 - (iii) a statement as to whether the international production order was issued on grounds relating to the investigation of one or more offences and, if so, the type or types of those offences; and
 - (iv) if subparagraph 30(2)(g)(ii) or (h)(ii) applied to the order—a statement to that effect; and
 - (v) if subparagraph 60(2)(g)(ii) or (h)(ii) applied to the order—a statement to that effect; and
 - (vi) if a period was specified in the order—details of that period; and
 - (vii) a record of the agency giving the order, or a certified copy of the order, to the Australian Designated Authority; and
 - (viii) details of each communication by an officer of the agency to a person other than an officer of the agency of

Clause 134

- protected information obtained in accordance with the order; and
- (ix) a record of the prescribed communications provider to whom the order was directed; and
 - (x) a statement as to whether the prescribed communications provider complied with the order; and
 - (xi) if the prescribed communications provider made intercepted communications, messages, voice calls or video calls available to the agency directly—a statement to that effect; and
 - (xii) if the prescribed communications provider made stored communications or telecommunications data available to the agency directly—a statement to that effect; and
 - (xiii) if the agency used protected information obtained in accordance with the order—a statement setting out details of that use of the protected information; and
 - (xiv) if the chief officer revoked the order under clause 114—a statement setting out the reasons for the revocation; and
 - (xv) if the Australian Designated Authority cancelled the order under clause 122—a record of the cancellation; and
 - (xvi) if a certifying officer of the agency certified a document to be a true copy of the order—a statement to that effect;
- (d) documents indicating whether a record was destroyed in accordance with subclause 140(1) or (3);
- (e) documents and other materials of a kind prescribed under subclause (2).
- (2) The Minister may, by legislative instrument, prescribe kinds of documents and other materials that the chief officer of a relevant agency must cause to be kept in the agency's records.
- (3) The period for which the chief officer of a relevant agency must cause a particular item to be kept in the agency's records under subclause (1) is the period:

- (a) starting when the item came into existence; and
 - (b) ending:
 - (i) when 3 years have elapsed since the item came into existence; or
 - (ii) when the Ombudsman gives a report to the Minister under clause 150 that is about records that include the item;
- whichever happens earlier.

135 Keeping documents associated with international production orders—the Organisation

- (1) The Director-General of Security must cause the following to be kept in the Organisation's records:
 - (a) a copy of each written application made under Part 4 of this Schedule for an international production order;
 - (b) a copy of each affidavit that accompanied a written application under Part 4 of this Schedule for an international production order;
 - (ba) a copy of each written request that the Attorney-General consent orally to the making of an application under Part 4 of this Schedule for an international production order;
 - (bb) a copy of each written consent by the Attorney-General to the making of an application under Part 4 of this Schedule for an international production order;
 - (bc) a copy of each report given to the Attorney-General under subclause 83(9) or 92(9);
 - (bd) a copy of each document of a kind specified in a written agreement between the Director-General of Security and the Inspector-General of Intelligence and Security;
 - (c) a copy of each international production order issued under Part 4 of this Schedule;
 - (d) a copy of each authorisation given by the Director-General of Security under subclause 83(4);
 - (e) a copy of each authorisation given by the Director-General of Security under subclause 92(4);

Clause 136

- (f) a copy of each authorisation given by the Director-General of Security under subclause 101(4);
 - (g) if the Director-General of Security revoked an international production order under clause 116—a copy of the instrument of revocation.
- (2) The period for which the Director-General of Security must cause a copy of a particular document to be kept in the Organisation's records under subclause (1) is the period:
- (a) starting when the document came into existence; and
 - (b) if:
 - (i) the document relates to an international production order that was issued under Part 4 of this Schedule; and
 - (ii) information was obtained in accordance with the order; ending at the later of the following times:
 - (iii) when 3 years have elapsed since the document came into existence;
 - (iv) when the Organisation ceases to retain the information that was obtained in accordance with the order; and
 - (c) if paragraph (b) does not apply—ending when 3 years have elapsed since the document came into existence.
- (3) An agreement under paragraph (1)(bd) is not a legislative instrument.

136 Other records to be kept—the Organisation

- (1) The Director-General of Security must cause the following to be kept in the Organisation's records:
- (a) details of each telephone application made under Part 4 of this Schedule for an international production order;
 - (b) for each application made under Part 4 of this Schedule for an international production order—a statement as to whether the application was granted, refused or withdrawn;
 - (ba) a record of each oral request that the Attorney-General consent orally to the making of an application under Part 4 of this Schedule for an international production order;

- (bb) a record of each oral consent by the Attorney-General to the making of an application under Part 4 of this Schedule for an international production order;
- (bc) each record of a kind specified in a written agreement between the Director-General of Security and the Inspector-General of Intelligence and Security;
- (c) for each international production order issued under Part 4 of this Schedule:
 - (i) a record of the type of order; and
 - (ii) a record of the designated international agreement nominated in the application for the order; and
 - (iii) if a period was specified in the order—details of that period; and
 - (iv) a record of the Organisation giving the order, or a certified copy of the order, to the Australian Designated Authority; and
 - (v) details of each communication by an ASIO official to a person other than an ASIO official of protected information obtained in accordance with the order; and
 - (vi) a record of the prescribed communications provider to whom the order was directed; and
 - (vii) a statement as to whether the prescribed communications provider complied with the order; and
 - (viii) if the prescribed communications provider made intercepted communications, messages, voice calls, video calls, stored communications or telecommunications data available to the Organisation directly—a statement to that effect; and
 - (ix) if the Organisation used protected information obtained in accordance with the order—a statement setting out details of that use of the protected information; and
 - (x) if the Director-General of Security revokes the order under clause 116—a statement setting out the reasons for the revocation; and

Clause 137

- (xi) if the Australian Designated Authority cancelled the order under clause 122—a record of the cancellation; and
 - (xii) if a certifying person certified a document to be a true copy of the order—a statement to that effect;
 - (d) documents indicating whether a record was destroyed in accordance with subclause 140(2) or (4).
- (2) The period for which the Director-General of Security must cause a particular record to be kept in the Organisation’s records under subclause (1) is the period:
- (a) starting when the record came into existence; and
 - (b) if:
 - (i) the record relates to an international production order that was issued under Part 4 of this Schedule; and
 - (ii) information was obtained in accordance with the order; ending at the later of the following times:
 - (iii) when 3 years have elapsed since the record came into existence;
 - (iv) when the Organisation ceases to retain the information that was obtained in accordance with the order; and
 - (c) if paragraph (b) does not apply—ending when 3 years have elapsed since the record came into existence.
- (3) An agreement under paragraph (1)(bc) is not a legislative instrument.

137 Keeping documents associated with international production orders—Australian Designated Authority

- (1) The Australian Designated authority must cause the following to be kept in the Australian Designated Authority’s records:
- (a) a copy of each international production order given by the Australian Designated Authority to a prescribed communications provider;
 - (b) if an instrument of revocation of an international production order was given by the Australian Designated Authority to a

- prescribed communications provider—a copy of the instrument of revocation;
- (c) if an instrument of cancellation of an international production order was given by the Australian Designated Authority to a prescribed communications provider—a copy of the instrument of cancellation;
 - (d) a copy of each objection received by the Australian Designated Authority under clause 121.
- (2) The period for which the Australian Designated Authority must cause a document to be kept in the Australian Designated Authority's records under subclause (1) is the period:
- (a) starting when the document came into existence; and
 - (b) ending when 3 years have elapsed since the document came into existence.

138 Other records to be kept—Australian Designated Authority

- (1) The Australian Designated Authority must cause the following to be kept in the Australian Designated Authority's records:
- (a) for each international production order given by the Australian Designated Authority to a prescribed communications provider:
 - (i) a record of the type of order; and
 - (ii) a record of the Australian entity that applied for the order; and
 - (iii) the name of the designated international agreement invoked by the order; and
 - (iv) the name of the prescribed communications provider; and
 - (v) if, in compliance with the order, the prescribed communications provider made intercepted communications, messages, voice calls or video calls available to an Australian entity directly—a statement to that effect; and
 - (vi) if, in compliance with the order, the prescribed communications provider made stored communications

Clause 138

- or telecommunications data available to an Australian entity directly—a statement to that effect;
- (b) if an international production order is cancelled by the Australian Designated Authority under clause 111, 112 or 122—a record of the cancellation and the reasons for the cancellation;
 - (c) if an instrument of revocation of an international production order is given by the Australian Designated Authority to a prescribed communications provider—a record of the giving of the instrument;
 - (d) if an instrument of cancellation of an international production order is given by the Australian Designated Authority to a prescribed communications provider—a record of the giving of the instrument;
 - (e) if an objection is received by the Australian Designated Authority under clause 121:
 - (i) a record of the receipt of the objection; and
 - (ii) a record of the international production order to which the objection relates; and
 - (iii) a record of the type of order; and
 - (iv) the name of the designated international agreement invoked by the order; and
 - (v) the name of the prescribed communications provider to whom the order is directed; and
 - (vi) the name of the Australian entity that applied for the order; and
 - (vii) if the objection was referred to an authority (however described) of a foreign country—a record of the referral.
- (2) If:
- (a) there is a designated international agreement between Australia and one or more foreign countries; and
 - (b) the agreement deals with (among other things) the issue of orders (however described) by a competent authority (however described) of such a foreign country; and

- (c) such an order (the *incoming order*) is directed to a prescribed communications provider that:
 - (i) carries on activities in Australia; or
 - (ii) provides one or more services to end-users who are physically present in Australia; and
 - (d) the provider notifies an authority (however described) of the foreign country that the provider objects to the incoming order:
 - (i) on the grounds that the incoming order does not comply with the designated international agreement; or
 - (ii) on similar grounds; and
 - (e) the Australian Designated Authority is aware of the objection;
- the Australian Designated Authority must cause the following to be kept in the Australian Designated Authority's records:
- (f) a record of the objection;
 - (g) the name of the foreign entity that applied for the incoming order;
 - (h) the name of the designated international agreement;
 - (i) the name of the provider;
 - (j) a record of whether the incoming order was cancelled (however described), withdrawn or set aside as a result of the objection;
 - (k) if the Australian Designated Authority made one or more representations to an authority (however described) of the foreign country that resulted in the incoming order being cancelled (however described), withdrawn or set aside—a record of those representations.
- (3) The period for which the Australian Designated Authority must cause a particular record to be kept in the Australian Designated Authority's records under subclause (1) or (2) is the period:
- (a) starting when the record came into existence; and
 - (b) ending when 3 years have elapsed since the record came into existence.

Clause 138

- (4) For the purposes of this clause, *Australian entity* means:
 - (a) a relevant agency; or
 - (b) the Organisation.
- (5) For the purposes of this clause, *foreign entity* means an agency or authority of a foreign country.

Division 4—Register of international production orders

139 Register of international production orders

- (1) The Australian Designated Authority must cause to be kept a register of international production orders.
- (2) The Australian Designated Authority must cause each of the following to be recorded in the register in relation to each international production order:
 - (a) the date of issue of the order;
 - (b) the type of order;
 - (c) particulars of the person who issued the order;
 - (d) if a relevant agency applied for the order—the name of the relevant agency;
 - (e) if the order was issued under Part 4 of this Schedule—the fact that the Organisation applied for the order;
 - (f) the name of the prescribed communications provider to whom the order is directed;
 - (g) the name of the designated international agreement nominated in the application for the order;
 - (h) if the order was issued under clause 30—the period that was specified in the order for the purposes of subparagraph 30(2)(i)(i) or (j)(i);
 - (i) if the order was issued under clause 60—the period that was specified in the order for the purposes of subparagraph 60(2)(k)(i) or (l)(i);
 - (j) if the order was issued under clause 89—the period that was specified in the order for the purposes of subparagraph 89(2)(i)(i) or (j)(i);
 - (k) if:
 - (i) the order was issued under clause 48; and
 - (ii) a period was specified in the order for the purposes of paragraph 48(2)(f);that period;

Clause 139

- (l) if:
 - (i) the order was issued under clause 78; and
 - (ii) a period was specified in the order for the purposes of paragraph 78(2)(g);that period;
 - (m) if:
 - (i) the order was issued under clause 107; and
 - (ii) a period was specified in the order for the purposes of paragraph 107(2)(f);that period;
 - (n) if the order was issued under Part 2 of this Schedule in response to an application made on grounds relating to the investigation of one or more offences—the type or types of those offences;
 - (o) if the order was issued under Part 3 of this Schedule in relation to a Part 5.3 supervisory order—the name of the person to whom the Part 5.3 supervisory order relates.
- (3) An IGIS official may access information in the register for the purposes of the performance of a function or duty, or the exercise of a power, by the IGIS official.

Division 5—Destruction of records

140 Destruction of records

Interception

- (1) If:
- (a) an international production order was issued in response to an application made by a relevant agency; and
 - (b) in compliance with the order, a prescribed communications provider makes:
 - (i) intercepted communications; or
 - (ii) intercepted messages; or
 - (iii) intercepted voice calls; or
 - (iv) intercepted video calls;available to the agency (whether directly or indirectly via the Australian Designated Authority); and
 - (c) a record of the intercepted communications, intercepted messages, intercepted voice calls, or intercepted video calls, as the case may be, is in the agency's possession; and
 - (d) the chief officer of the agency is satisfied that the record is not likely to be required for a purpose referred to in clause 153 or 157;
- the chief officer must cause the record to be destroyed immediately after becoming so satisfied.
- (2) If:
- (a) an international production order was issued under clause 89; and
 - (b) in compliance with the order, a prescribed communications provider makes:
 - (i) intercepted communications; or
 - (ii) intercepted messages; or
 - (iii) intercepted voice calls; or
 - (iv) intercepted video calls;

Clause 140

available to the Organisation (whether directly or indirectly via the Australian Designated Authority); and

- (c) a record of the intercepted communications, intercepted messages, intercepted voice calls, or intercepted video calls, as the case may be, is in the Organisation's possession; and
- (d) the Director-General of Security is satisfied that the record is not likely to be required for a purpose referred to in clause 153 or 157;

the Director-General of Security must cause the record to be destroyed immediately after becoming so satisfied.

Stored communications

(3) If:

- (a) an international production order was issued in response to an application made by a relevant agency; and
- (b) in compliance with the order, a prescribed communications provider makes a copy of stored communications available to the agency (whether directly or indirectly via the Australian Designated Authority); and
- (c) the copy is in the agency's possession; and
- (d) the chief officer of the agency is satisfied that the copy is not likely to be required for a purpose referred to in clause 153 or 158;

the chief officer must cause the copy to be destroyed immediately after becoming so satisfied.

(4) If:

- (a) an international production order was issued under clause 98; and
- (b) in compliance with the order, a prescribed communications provider makes a copy of stored communications available to the Organisation (whether directly or indirectly via the Australian Designated Authority); and
- (c) the copy is in the Organisation's possession; and

(d) the Director-General of Security is satisfied that the copy is not likely to be required for a purpose referred to in clause 153 or 158;
the Director-General of Security must cause the copy to be destroyed immediately after becoming so satisfied.

Part 10—Oversight by the Commonwealth Ombudsman

141 Simplified outline of this Part

- The Ombudsman may inspect records of a relevant agency to determine the extent of compliance with this Schedule by the relevant agency and its officers.
- The Ombudsman may inspect records of the Australian Designated Authority to determine the extent of compliance with this Schedule by the Australian Designated Authority.
- The Ombudsman must give the Minister an annual report about the results of those inspections.

142 Inspection of records—relevant agency

- (1) The Ombudsman may inspect records of a relevant agency to determine the extent of compliance with this Schedule by the relevant agency and its officers.
- (2) For the purpose of an inspection under this clause, the Ombudsman:
 - (a) after notifying the chief officer of the relevant agency, may enter at any reasonable time premises occupied by the relevant agency; and
 - (b) is entitled to have full and free access at all reasonable times to all records of the relevant agency that are relevant to the inspection; and
 - (c) despite any other law, is entitled to make copies of, and to take extracts from, records of the relevant agency; and

- (d) may require a member of staff of the relevant agency to give the Ombudsman any information that the Ombudsman considers necessary, being information:
 - (i) that is in the member's possession, or to which the member has access; and
 - (ii) that is relevant to the inspection.
- (3) Before inspecting records of a relevant agency under this clause, the Ombudsman must give reasonable notice to the chief officer of the relevant agency of when the inspection will occur.
- (4) The chief officer must ensure that members of staff of the relevant agency give the Ombudsman any assistance the Ombudsman reasonably requires to enable the Ombudsman to perform functions under this clause.

143 Inspection of records—Australian Designated Authority

- (1) The Ombudsman may inspect records of the Australian Designated Authority to determine the extent of compliance with this Schedule by the Australian Designated Authority.
- (2) For the purpose of an inspection under this clause, the Ombudsman:
 - (a) after notifying the Australian Designated Authority, may enter at any reasonable time premises occupied by the Attorney-General's Department; and
 - (b) is entitled to have full and free access at all reasonable times to all records of the Australian Designated Authority that are relevant to the inspection; and
 - (c) despite any other law, is entitled to make copies of, and to take extracts from, records of the Australian Designated Authority; and
 - (d) may require a member of staff of the Attorney-General's Department to give the Ombudsman any information that the Ombudsman considers necessary, being information:
 - (i) that is in the member's possession, or to which the member has access; and

Clause 144

- (ii) that is relevant to the inspection.
- (3) Before inspecting records of the Australian Designated Authority under this clause, the Ombudsman must give reasonable notice to the Australian Designated Authority of when the inspection will occur.
- (4) The Australian Designated Authority must ensure that members of staff of the Attorney-General's Department give the Ombudsman any assistance the Ombudsman reasonably requires to enable the Ombudsman to perform functions under this clause.

144 Power to obtain relevant information

Relevant agency

- (1) If the Ombudsman has reasonable grounds to believe that an officer of a particular relevant agency is able to give information relevant to an inspection under this Part of the relevant agency's records, the Ombudsman may:
 - (a) if the Ombudsman knows the officer's identity—by written notice given to the officer, require the officer to do one or both of the following:
 - (i) give the information to the Ombudsman, by writing signed by the officer, at a specified place and within a specified period;
 - (ii) attend before a specified inspecting officer to answer questions relevant to the inspection; or
 - (b) if the Ombudsman does not know the officer's identity—require the chief officer of the relevant agency, or a person nominated by the chief officer, to attend before a specified inspecting officer to answer questions relevant to the inspection.

Australian Designated Authority

- (2) If the Ombudsman has reasonable grounds to believe that a member of staff of the Attorney-General's Department is able to

give information relevant to an inspection under this Part of the Australian Designated Authority's records, the Ombudsman may:

- (a) if the Ombudsman knows the member's identity—by written notice given to the member, require the member to do one or both of the following:
 - (i) give the information to the Ombudsman, by writing signed by the member, at a specified place and within a specified period;
 - (ii) attend before a specified inspecting officer to answer questions relevant to the inspection; or
- (b) if the Ombudsman does not know the member's identity—require the Australian Designated Authority, or a person nominated by the Australian Designated Authority, to attend before a specified inspecting officer to answer questions relevant to the inspection.

Specification of place and period etc.

- (3) A requirement under subclause (1) or (2) to attend before an inspecting officer must specify:
 - (a) a place for the attendance; and
 - (b) a period within which, or a time and day when, the attendance is to occur.

The place, and the period or the time and day, must be reasonable having regard to the circumstances in which the requirement is made.

Offence

- (4) A person commits an offence if:
 - (a) the person is subject to a requirement under subclause (1) or (2); and
 - (b) the person omits to do an act; and
 - (c) the omission breaches the requirement.

Penalty for an offence against this subclause: Imprisonment
for 6 months.

Clause 145

145 Ombudsman to be given information and access despite other laws

- (1) Despite any other law, a person is not excused from giving information, answering a question, or giving access to a document, as and when required under this Part, on the ground that giving the information, answering the question, or giving access to the document, as the case may be:
 - (a) would contravene a law; or
 - (b) would be contrary to the public interest; or
 - (c) might tend to incriminate the person or make the person liable to a penalty.
- (2) However:
 - (a) the information, the answer, or the fact that the person has given access to the document, as the case may be; or
 - (b) any information or thing (including a document) obtained as a direct or indirect consequence of giving the information, answering the question or giving access to the document;is not admissible in evidence against the person except in a proceeding by way of a prosecution for:
 - (c) an offence against clause 152; or
 - (d) an offence against Part 7.4 or 7.7 of the *Criminal Code*.
- (3) Nothing in clause 152, or in any other law, prevents an officer of a relevant agency from:
 - (a) giving information to an inspecting officer (whether orally or in writing and whether or not in answer to a question); or
 - (b) giving access to a record of the relevant agency to an inspecting officer;for the purposes of an inspection under this Part of the relevant agency's records.
- (4) Nothing in clause 152, or in any other law, prevents an officer of a relevant agency from making a record of information, or causing a record of information to be made, for the purposes of giving the information to a person as permitted by subclause (3).

- (5) Nothing in clause 152, or in any other law, prevents a member of staff of the Attorney-General's Department from:
- (a) giving information to an inspecting officer (whether orally or in writing and whether or not in answer to a question); or
 - (b) giving access to a record of the Australian Designated Authority to an inspecting officer;
- for the purposes of an inspection under this Part of the Australian Designated Authority's records.
- (6) Nothing in clause 152, or in any other law, prevents a member of staff of the Attorney-General's Department from making a record of information, or causing a record of information to be made, for the purposes of giving the information to a person as permitted by subclause (5).

146 Application of Ombudsman Act

- (1) Section 11A of the *Ombudsman Act 1976* does not apply in relation to the exercise or proposed exercise of a power, or the performance or the proposed performance of a function, of the Ombudsman under this Part.
- (2) A reference in section 19 of the *Ombudsman Act 1976* to the Ombudsman's operations does not include a reference to anything that an inspecting officer has done or omitted to do under this Part.
- (3) Subject to clause 145, subsections 35(2), (3), (4) and (8) of the *Ombudsman Act 1976* apply for the purposes of this Part and so apply as if:
- (a) a reference in those subsections to an officer were a reference to an inspecting officer; and
 - (b) a reference in those subsections to information did not include a reference to protected information; and
 - (c) a reference in those subsections to that Act were a reference to this Part; and
 - (d) paragraph 35(3)(b) of that Act were omitted; and
 - (e) section 35A of that Act had not been enacted.

Clause 147

147 Exchange of information between Ombudsman and State/Territory inspecting authorities

- (1) If the Ombudsman has obtained under this Part information relating to an authority of a State or Territory, the Ombudsman may give the information to another authority of that State or Territory (an *inspecting authority*) that:
 - (a) has powers under the law of that State or Territory; and
 - (b) has the function of making inspections of a similar kind to those provided for in clause 142 when the inspecting authority is exercising those powers.
- (2) However, the Ombudsman may give the information only if the Ombudsman is satisfied that giving the information is necessary to enable the inspecting authority to perform its functions in relation to the first-mentioned authority of the State or Territory.
- (3) An inspecting authority may give the Ombudsman information relevant to the performance of the Ombudsman's functions under this Part.

148 Delegation by Ombudsman

- (1) The Ombudsman may, by writing, delegate:
 - (a) to an APS employee responsible to the Ombudsman; or
 - (b) to a person having similar oversight functions to the Ombudsman under the law of a State or Territory or to an employee responsible to that person;all or any of the Ombudsman's powers under this Part other than a power to report to the Minister.
- (2) A delegate must, upon request by a person affected by the exercise of any power delegated to the delegate, produce the instrument of delegation, or a copy of the instrument, for inspection by the person.

149 Ombudsman not to be sued

The Ombudsman, an inspecting officer, or a person acting under an inspecting officer's direction or authority, is not liable to an action, suit or proceeding for or in relation to an act done, or omitted to be done, in good faith in the performance or exercise, or the purported performance or exercise, of a function or power conferred by this Part.

150 Reports

- (1) The Ombudsman must report to the Minister, in writing, about the results of:
 - (a) inspections under clause 142 of the records of relevant agencies during a financial year; and
 - (b) inspections under clause 143 of the records of the Australian Designated Authority during a financial year.
- (2) The report under subclause (1) must be given to the Minister as soon as practicable after the end of the financial year.
- (3) The Minister must cause a copy of the report to be tabled in each House of the Parliament within 15 sitting days of that House after the Minister receives it.
- (4) The Ombudsman may report to the Minister in writing at any time about the results of an inspection under this Part and must do so if so requested by the Minister.
- (5) If, as a result of an inspection under this Part of the records of a relevant agency, the Ombudsman is of the opinion that an officer of the relevant agency has contravened a provision of this Schedule, the Ombudsman may include in the Ombudsman's report on the inspection a report on the contravention.
- (6) If, as a result of an inspection under this Part of the records of the Australian Designated Authority, the Ombudsman is of the opinion that a member of staff of the Attorney-General's Department has contravened a provision of this Schedule, the Ombudsman may

Clause 150

include in the Ombudsman's report on the inspection a report on the contravention.

- (7) The Ombudsman must:
- (a) give the chief officer of a relevant agency a copy of so much of a report under subclause (1) or (4) as relates to the relevant agency; and
 - (b) give the Australian Designated Authority a copy of so much of a report under subclause (1) or (4) as relates to the Australian Designated Authority.
- (8) A report under this clause must not include information which, if made public, could reasonably be expected to:
- (a) endanger a person's safety; or
 - (b) prejudice an investigation or prosecution; or
 - (c) compromise any relevant agency's operational activities or methodologies.

Part 11—Disclosure of protected information

151 Simplified outline of this Part

- Protected information must not be used, recorded or disclosed, unless an exception applies.
- Protected information must not be admitted in evidence, unless an exception applies.

152 Prohibition on use, recording or disclosure of protected information or its admission in evidence

- (1) A person commits an offence if:
 - (a) the person uses, records or discloses information; and
 - (b) the information is protected information; and
 - (c) the use, recording or disclosure of the information is not permitted by this Part.

Penalty: Imprisonment for 2 years.

- (2) Subject to this Part, protected information must not be admitted in evidence in any proceedings in Australia.

153 Exceptions—general

- (1) Protected information may be used, recorded or disclosed, or may be admitted in evidence, for any of the following purposes:
 - (a) the investigation of a serious category 1 offence or a serious category 2 offence or the making of a report on the outcome of such an investigation;
 - (b) the making of a decision whether or not to bring a prosecution for a serious category 1 offence or a serious category 2 offence (other than an offence referred to in paragraph (r));

Clause 153

- (c) a proceeding by way of a prosecution for a serious category 1 offence or a serious category 2 offence (other than an offence referred to in paragraph (r));
- (d) a proceeding by way of a bail application if the application relates to a proceeding by way of a prosecution for a serious category 1 offence or a serious category 2 offence;
- (e) a proceeding by way of review of a decision to refuse such a bail application;
- (f) a proceeding by way of a review of a decision to grant such a bail application;
- (g) the investigation of a contravention of a civil penalty provision in this Schedule or the making of a report on the outcome of such an investigation;
- (h) the performance of the functions, or the exercise of the powers, of the Organisation;
- (i) the performance of a function or duty, or the exercise of a power, by a person, court or other body under, or in relation to a matter arising under, Division 104 (control orders) or Division 105A (post-sentence orders) of the *Criminal Code*;
- (j) a preventative detention order law;
- (k) a post-sentence detention law or a post-sentence supervision law;
- (ka) the making of a decision whether to apply for a post-sentence order, or for a variation or review of a post-sentence order, under Division 105A of the *Criminal Code* in relation to a person;
- (kb) the making of a decision whether to apply for an order, or make any other application in relation to an order, under a post-sentence detention law or a post-sentence supervision law in relation to a person;
- (l) a proceeding by way of an application for a civil penalty order in relation to a contravention of a civil penalty provision in this Schedule;
- (m) the making of reports, and the keeping of records, under Part 9 of this Schedule;

- (n) the making of reports referred to in subsection 94(1) of the *Australian Security Intelligence Organisation Act 1979*, so far as they include statements covered by subsection 94(2BBA) of that Act;
- (o) an inspection by the Ombudsman under clause 142 or 143;
- (p) the performance of a function or duty, or the exercise of a power, by an IGIS official;
- (q) the performance of a function or duty, or the exercise of a power, by an Ombudsman official;
- (r) an investigation under the *Privacy Act 1988* or any other law of the Commonwealth concerning the privacy of personal information and also any subsequent investigation or prosecution of a serious category 1 offence, or a serious category 2 offence, arising directly from that first-mentioned investigation;
- (s) the administration or execution of this Schedule;
- (t) any legal proceedings arising out of or otherwise related to this Schedule or any report of any such proceedings;
- (u) a proceeding for the taking of evidence pursuant to section 43 of the *Extradition Act 1988*, in so far as the proceeding relates to a serious category 1 offence;
- (v) a proceeding under section 13 of the *Mutual Assistance in Criminal Matters Act 1987* in relation to a criminal matter (within the meaning of that Act) that concerns an offence, against the laws of the foreign country that made the request resulting in the proceeding, that is punishable by imprisonment for life or for a period, or maximum period, of at least 3 years;
- (w) a proceeding under Division 5 of Part 4 of the *International Criminal Court Act 2002*;
- (x) a proceeding before the International Criminal Court sitting in Australia under Part 5 of the *International Criminal Court Act 2002*;
- (y) a proceeding under Division 1 of Part 4 of the *International War Crimes Tribunals Act 1995*;
- (z) a designated international agreement.

Clause 153

- (2) For the purposes of subclause (1), **this Schedule** includes the *Regulatory Powers (Standard Provisions) Act 2014*, so far as that Act relates to this Schedule.

Disclosure to Public Interest Monitor of Victoria or Queensland

- (3) If:
- (a) a person (the **applicant**) applies, or proposes to apply, under clause 22, on behalf of an interception agency of Victoria or Queensland for an international production order under clause 30; and
 - (b) a law of that State authorises or requires the applicant:
 - (i) to notify a PIM of that State of the application or proposed application; or
 - (ii) to notify a PIM of that State of any information that relates to the application or proposed application; or
 - (iii) to give a PIM of that State any document that relates to the application or proposed application;making the notification, or giving the document, to a PIM of that State is taken to be necessary for the purposes of the administration or execution of this Schedule.

- (4) If:
- (a) a person (the **applicant**) applies, or proposes to apply, under clause 52, on behalf of a Part 5.3 IPO agency of Victoria or Queensland for an international production order under clause 60; and
 - (b) a law of that State authorises or requires the applicant:
 - (i) to notify a PIM of that State of the application or proposed application; or
 - (ii) to notify a PIM of that State of any information that relates to the application or proposed application; or
 - (iii) to give a PIM of that State any document that relates to the application or proposed application;making the notification, or giving the document, to a PIM of that State is taken to be necessary for the purposes of the administration or execution of this Schedule.

International assistance

- (5) If the Attorney-General has authorised the provision of protected information to a foreign country under subsection 13A(1) of the *Mutual Assistance in Criminal Matters Act 1987*, the information may be disclosed to:
- (a) that foreign country; or
 - (b) the Secretary of the Attorney-General's Department for the purpose of providing the information to that foreign country.
- (6) If the Attorney-General has authorised the provision of protected information to the International Criminal Court under section 69A of the *International Criminal Court Act 2002*, the information may be disclosed to:
- (a) that Court; or
 - (b) the Secretary of the Attorney-General's Department for the purpose of providing the information to that Court.
- (7) If the Attorney-General has authorised the provision of protected information to a War Crimes Tribunal under section 25A of the *International War Crimes Tribunals Act 1995*, the information may be disclosed to:
- (a) that Tribunal; or
 - (b) the Secretary of the Attorney-General's Department for the purpose of providing the information to that Tribunal.

154 Exception—disclosure to the Minister

Protected information may be disclosed to the Minister for the purposes of the performance of the functions, or the exercise of the powers, of the Minister.

155 Exception—disclosure to the Attorney-General

Protected information may be disclosed to the Attorney-General for the purposes of the performance of the functions, or the exercise of the powers, of the Attorney-General.

Clause 156

156 Exception—statistical information

A prescribed communications provider may disclose the total number of international production orders given to the provider during a period of at least 6 months.

Note: This clause authorises the disclosure of aggregate statistical information. That information cannot be broken down:

- (a) by agency; or
- (b) in any other way.

157 Exceptions—international production orders relating to interception

- (1) Protected information that:
- (a) was obtained in accordance with an international production order issued under clause 30, 60 or 89; or
 - (b) relates to an international production order issued under clause 30, 60 or 89;
- may be used, recorded or disclosed, or may be admitted in evidence, for any of the following purposes:
- (c) a proceeding for the confiscation or forfeiture of property in connection with the commission of a serious category 1 offence;
 - (d) a proceeding under the *Spam Act 2003*;
 - (e) a proceeding under, or a proceeding relating to a matter arising under, the main unexplained wealth provisions;
 - (f) a proceeding under, or a proceeding relating to a matter arising under, the unexplained wealth legislation of a participating State, the Australian Capital Territory or the Northern Territory;
 - (g) a proceeding under, or a proceeding relating to a matter arising under, an organised crime control law;
 - (h) a proceeding for the extradition of a person from a State or Territory to another State or Territory, in so far as the proceeding relates to a serious category 1 offence;

- (i) a proceeding by way of a coroner's inquest if, in the opinion of the coroner, the event that is the subject of the inquest may have resulted from the commission of a serious category 1 offence;
- (j) a police disciplinary proceeding;
- (k) a proceeding in so far as it relates to:
 - (i) a decision by the Commissioner of Police to terminate the employment of an AFP employee or the appointment of a special member of the Australian Federal Police; or
 - (ii) a decision by the Commissioner of a Police Force of a State to terminate the appointment of an officer or member of staff of that Police Force;
- (l) a proceeding in so far as it is, or relates to, disciplinary or legal action (within the meaning of section 6S) that is in relation to an eligible staff member (within the meaning of that section) of the Australian Federal Police or the ACC;
- (m) any other proceeding (not being a proceeding by way of a prosecution for an offence) in so far as it relates to alleged misbehaviour, or alleged improper conduct, of an officer of the Commonwealth or of a State;
- (n) a proceeding for the recovery of an amount due to a network entity or transmission service provider in connection with the supply of a transmission service;
- (o) a proceeding of an eligible Commonwealth authority;
- (p) a proceeding of the Independent Commission Against Corruption;
- (q) a proceeding of the Inspector of the Independent Commission Against Corruption;
- (r) a proceeding in relation to an application under subsection 34B(1) of the ACC Act in respect of contempt of the ACC;
- (s) a proceeding of the IBAC;
- (t) a proceeding of the Victorian Inspectorate;
- (u) a proceeding of the Corruption and Crime Commission;

Clause 157

- (v) a proceeding of the Parliamentary Inspector of the Corruption and Crime Commission;
- (w) a proceeding of the Law Enforcement Conduct Commission;
- (x) a proceeding of the Inspector of the Law Enforcement Conduct Commission;
- (y) a proceeding of the Crime and Corruption Commission;
- (z) a proceeding of the Independent Commissioner Against Corruption;
- (za) an eligible purpose of the ACC;
- (zb) an eligible purpose of the Australian Federal Police;
- (zc) an eligible purpose of the Australian Commission for Law Enforcement Integrity;
- (zd) an eligible purpose of a Commonwealth Royal Commission that is an eligible Commonwealth authority;
- (ze) an eligible purpose of the Police Force of a State;
- (zf) an eligible purpose of an eligible authority of a State;
- (zg) an eligible purpose of the Independent Commission Against Corruption;
- (zh) an eligible purpose of the Inspector of the Independent Commission Against Corruption;
- (zi) an eligible purpose of the Inspector of the Law Enforcement Conduct Commission;
- (zj) an eligible purpose of the Law Enforcement Conduct Commission;
- (zk) an eligible purpose of the IBAC;
- (zl) an eligible purpose of the Victorian Inspectorate;
- (zm) an eligible purpose of the Corruption and Crime Commission;
- (zn) an eligible purpose of the Crime and Corruption Commission;
- (zo) an eligible purpose of the Parliamentary Inspector of the Corruption and Crime Commission;
- (zp) an eligible purpose of the Independent Commissioner Against Corruption.

Eligible purpose

- (2) For the purposes of this clause:
- (a) each of the following is an ***eligible purpose*** of the ACC:
 - (i) a special ACC operation/investigation;
 - (ii) a report to the Board of the ACC on the outcome of such an operation or investigation;
 - (iii) an investigation of, or an inquiry into, alleged misbehaviour, or alleged improper conduct, of a member of the staff referred to in subsection 47(1) of the ACC Act;
 - (iv) a report on such an investigation or inquiry;
 - (v) the making by a person of a decision, following such an investigation or inquiry, in relation to the employment of such a staff member (including a decision to terminate the staff member's employment);
 - (vi) a review (whether by way of appeal or otherwise) of such a decision; and
 - (b) each of the following is an ***eligible purpose*** of the Australian Federal Police:
 - (i) an investigation of, or an inquiry into, alleged misbehaviour, or alleged improper conduct, of an officer of the Commonwealth, being an investigation or inquiry under a law of the Commonwealth or by a person in the person's capacity as an officer of the Commonwealth;
 - (ii) a report on such an investigation or inquiry;
 - (iii) the making by a person of a decision under the *Australian Federal Police Act 1979* in relation to the engagement of an AFP employee, the retirement of an AFP employee or the termination of the employment of an AFP employee or in relation to the appointment or the termination of the appointment of a special member of the Australian Federal Police;
 - (iv) a review (whether by way of appeal or otherwise) of such a decision;

Clause 157

- (v) the tendering to the Governor-General of advice to terminate, because of misbehaviour or improper conduct, the appointment of an officer of the Commonwealth;
- (vi) deliberations of the Executive Council in connection with advice to the Governor-General to terminate, because of misbehaviour or improper conduct, the appointment of an officer of the Commonwealth; and
- (c) each of the following is an **eligible purpose** of the Australian Commission for Law Enforcement Integrity:
 - (i) a corruption investigation (within the meaning of the *Law Enforcement Integrity Commissioner Act 2006*);
 - (ii) a report on such an investigation; and
- (d) each of the following is an **eligible purpose** of a Commonwealth Royal Commission that is an eligible Commonwealth authority:
 - (i) an investigation that the Commonwealth Royal Commission is conducting in the course of the inquiry it is commissioned to undertake;
 - (ii) a report on such an investigation; and
- (e) each of the following is an **eligible purpose** of the Police Force of a State:
 - (i) an investigation of, or an inquiry into, alleged misbehaviour, or alleged improper conduct, of an officer of that State, being an investigation or inquiry under a law of that State or by a person in the person's capacity as an officer of that State;
 - (ii) a report on such an investigation or inquiry;
 - (iii) the making by a person of a decision in relation to the appointment, re-appointment, term of appointment, retirement or termination of appointment of an officer or member of staff of that Police Force;
 - (iv) a review (whether by way of appeal or otherwise) of such a decision;

- (v) the tendering to the Governor of that State of advice to terminate, because of misbehaviour or improper conduct, the appointment of an officer of that State;
- (vi) deliberations of the Executive Council of that State in connection with advice to the Governor of that State to terminate, because of misbehaviour or improper conduct, the appointment of an officer of that State; and
- (f) each of the following is an **eligible purpose** of an eligible authority of a State:
 - (i) an inspection of the authority's records that is made under a requirement of the law of that State, being a requirement of the kind referred to in paragraph 35(1)(h);
 - (ii) a report on such an inspection; and
- (g) each of the following is an **eligible purpose** of the Independent Commission Against Corruption:
 - (i) an investigation under the Independent Commission Against Corruption Act into whether corrupt conduct (within the meaning of that Act) may have occurred, may be occurring or may be about to occur;
 - (ii) a report on such an investigation; and
- (h) each of the following is an **eligible purpose** of the Inspector of the Independent Commission Against Corruption:
 - (i) dealing with (by reports and recommendations) complaints of abuse of power, impropriety or other forms of misconduct (within the meaning of the Independent Commission Against Corruption Act) on the part of the Independent Commission Against Corruption or officers of that Commission;
 - (ii) dealing with (by reports and recommendations) conduct amounting to maladministration (within the meaning of the Independent Commission Against Corruption Act) by the Independent Commission Against Corruption or officers of that Commission; and
- (i) each of the following is an **eligible purpose** of the Inspector of the Law Enforcement Conduct Commission:

Clause 157

- (i) dealing with (by reports and recommendations) conduct amounting to agency maladministration (within the meaning of subsection 5(6A)) on the part of the Commission (whether or not the subject of a complaint);
- (ii) dealing with (by reports and recommendations) conduct amounting to officer misconduct (within the meaning of section 122 of the *Law Enforcement Conduct Commission Act 2016* (NSW)) or officer maladministration (within the meaning of that section) on the part of officers (within the meaning of that Act) of the Commission (whether or not the subject of a complaint); and
- (j) each of the following is an **eligible purpose** of the Law Enforcement Conduct Commission:
 - (i) an investigation under Part 6 of the *Law Enforcement Conduct Commission Act 2016* (NSW) in respect of conduct to which subsection 5(7) of this Act applies;
 - (ii) a report on an investigation covered by subparagraph (i);
 - (iii) the tendering to the Governor of New South Wales of advice to terminate, because of misbehaviour or improper conduct, the appointment of the Commissioner of the New South Wales Police Force;
 - (iv) deliberations of the Executive Council of New South Wales in connection with advice to the Governor of that State to terminate, because of misbehaviour or improper conduct, the appointment of the Commissioner of the New South Wales Police Force; and
- (k) each of the following is an **eligible purpose** of the IBAC:
 - (i) an investigation under the IBAC Act of corrupt conduct (within the meaning of that Act);
 - (ii) an investigation under the IBAC Act of police personnel conduct (within the meaning of that Act); and
- (l) each of the following is an **eligible purpose** of the Victorian Inspectorate:
 - (i) an investigation under the Victorian Inspectorate Act;

- (ii) a report or recommendation on such an investigation;
and
- (m) each of the following is an **eligible purpose** of the Corruption and Crime Commission:
 - (i) an investigation under the Corruption and Crime Commission Act into whether misconduct (within the meaning of that Act) has or may have occurred, is or may be occurring, is or may be about to occur, or is likely to occur;
 - (ii) a report on such an investigation; and
- (n) each of the following is an **eligible purpose** of the Crime and Corruption Commission:
 - (i) an investigation under the Crime and Corruption Act into whether corruption (within the meaning of that Act) may have occurred, may be occurring or may be about to occur;
 - (ii) a report on such an investigation; and
- (o) each of the following is an **eligible purpose** of the Parliamentary Inspector of the Corruption and Crime Commission:
 - (i) dealing with a matter of misconduct (within the meaning of the Corruption and Crime Commission Act) on the part of the Corruption and Crime Commission;
 - (ii) dealing with a matter of misconduct (within the meaning of the Corruption and Crime Commission Act) on the part of an officer of the Corruption and Crime Commission;
 - (iii) dealing with a matter of misconduct (within the meaning of the Corruption and Crime Commission Act) on the part of an officer of the Parliamentary Inspector of the Corruption and Crime Commission; and
- (p) each of the following is an **eligible purpose** of the Independent Commissioner Against Corruption:
 - (i) an investigation under the Independent Commissioner Against Corruption Act into corruption in public administration (within the meaning of that Act);

Clause 158

- (ii) a report on such an investigation.

158 Exceptions—international production orders relating to stored communications

Protected information that:

- (a) was obtained in accordance with an international production order issued under clause 39, 69 or 98; or
- (b) relates to an international production order issued under clause 39, 69 or 98;

may be used, recorded or disclosed, or may be admitted in evidence, for any of the following purposes:

- (c) a proceeding for the confiscation or forfeiture of property in connection with the commission of a serious category 1 offence;
- (d) a proceeding for the extradition of a person from a State or Territory to another State or Territory, in so far as the proceeding relates to a serious category 1 offence;
- (e) a proceeding by way of a coroner's inquest if, in the opinion of the coroner, the event that is the subject of the inquest may have resulted from the commission of a serious category 1 offence;
- (f) a proceeding for recovery of a pecuniary penalty for a contravention that would, if proved, render the person committing the contravention liable to:
 - (i) a pecuniary penalty, or a maximum pecuniary penalty, of at least 60 penalty units if the contravention is committed by an individual; or
 - (ii) if the contravention cannot be committed by an individual—a pecuniary penalty, or a maximum pecuniary penalty, of at least 300 penalty units;
- (g) a proceeding under the *Spam Act 2003*;
- (h) a police disciplinary proceeding.

159 Exceptions—telecommunications data

- (1) Protected information that:
 - (a) consists of telecommunications data obtained in accordance with an international production order; or
 - (b) relates to such an international production order; may be used, recorded or disclosed, or may be admitted in evidence, for any of the following purposes:
 - (c) the enforcement of the criminal law;
 - (d) the enforcement of a law imposing a pecuniary penalty;
 - (e) the protection of the public revenue.
- (2) If the Australian Federal Police, or a Police Force of a State has been notified that a person is missing, protected information that consists of telecommunications data obtained in accordance with an international production order may be disclosed if:
 - (a) the disclosure is reasonably necessary for the purposes of finding the missing person; or
 - (b) the information is disclosed to the person who notified the Australian Federal Police, or a Police Force of a State, of the missing person and:
 - (i) the missing person consented to the disclosure; or
 - (ii) the missing person is unable to consent, and the disclosure is reasonably necessary to prevent a threat to the missing person's health, life or safety; or
 - (iii) the missing person is dead.

Part 12—Evidentiary certificates

160 Simplified outline of this Part

- A manager of a prescribed communications provider may issue an evidentiary certificate setting out facts with respect to acts or things done by the provider in order to comply with an international production order.
- A manager of a prescribed communications provider may issue an evidentiary certificate setting out facts with respect to acts or things done by the provider in order to voluntarily provide information in connection with an international production order.
- A certifying officer of a relevant agency may issue an evidentiary certificate setting out facts with respect to the receipt by the agency of information that was made available to the agency in accordance with an international production order.
- A certifying person may issue an evidentiary certificate setting out facts with respect to the receipt by the Organisation of information that was made available to the Organisation in accordance with an international production order.
- If an international production order requires information to be made available to a relevant agency or the Organisation indirectly via the Australian Designated Authority, the Australian Designated Authority may issue an evidentiary certificate setting out facts with respect to:
 - (a) the receipt by the Australian Designated Authority of the information; or

- (b) anything done by the Australian Designated Authority for the purposes of ensuring that the information was passed on to the agency or the Organisation.

161 Evidentiary certificates—compliance with international production orders by prescribed communications providers

- (1) If:
- (a) an international production order is directed to a prescribed communications provider; and
 - (b) the provider is not an individual;
- a manager of the provider may issue a written certificate signed by the manager setting out such facts as the manager considers relevant with respect to acts or things done by the provider in order to comply with the international production order.
- (2) If:
- (a) an international production order is directed to a prescribed communications provider; and
 - (b) the provider is an individual;
- the provider may issue a written certificate signed by the provider setting out such facts as the provider considers relevant with respect to acts or things done by the provider in order to comply with the international production order.
- (3) A document purporting to be a certificate issued under subclause (1) or (2):
- (a) is to be received in evidence in a proceeding in Australia without further proof; and
 - (b) in a proceeding in Australia, is conclusive evidence of the matters stated in the document.

Clause 162

162 Evidentiary certificates—voluntary provision of associated information by prescribed communications providers

Interception

- (1) If:
- (a) an international production order is directed to a prescribed communications provider; and
 - (b) the provider is not an individual; and
 - (c) either:
 - (i) the order requires the provider to intercept communications carried by one or more individual transmission services, and make those intercepted communications available to a relevant agency or the Organisation; or
 - (ii) the order requires the provider to intercept messages sent or received, voice calls made or received, or video calls made or received, using one or more individual message/call application services, and make those intercepted messages, voice calls or video calls available to a relevant agency or the Organisation;
- a manager of the provider may do either or both of the following:
- (d) issue a written certificate signed by the manager setting out such facts as the manager considers relevant with respect to acts or things done by the provider in order to voluntarily give the relevant agency or the Organisation (as the case may be) in connection with the international production order, information relating to:
 - (i) those individual transmission services or individual message/call application services (as the case may be); or
 - (ii) a person who uses, or is likely to use, those individual transmission services or individual message/call application services (as the case may be);
 - (e) issue a written certificate signed by the manager setting out such facts as the manager considers would assist in explaining:

- (i) the operation of those individual transmission services or individual message/call application services (as the case may be); or
 - (ii) the way in which the intercepted communications, intercepted messages, intercepted voice calls or intercepted video calls (as the case may be) were made available by the provider to the relevant agency or the Organisation (as the case may be).
- (2) If:
- (a) an international production order is directed to a prescribed communications provider; and
 - (b) the provider is an individual; and
 - (c) either:
 - (i) the order requires the provider to intercept communications carried by one or more individual transmission services, and make those intercepted communications available to a relevant agency or the Organisation; or
 - (ii) the order requires the provider to intercept messages sent or received, voice calls made or received, or video calls made or received, using one or more individual message/call application services, and make those intercepted messages, voice calls or video calls available to a relevant agency or the Organisation;
- the provider may do either or both of the following:
- (d) issue a written certificate signed by the provider setting out such facts as the provider considers relevant with respect to acts or things done by the provider in order to voluntarily give the relevant agency or the Organisation (as the case may be) in connection with the international production order, information relating to:
 - (i) those individual transmission services or individual message/call application services (as the case may be); or

Clause 162

- (ii) a person who uses, or is likely to use, those individual transmission services or individual message/call application services (as the case may be);
- (e) issue a written certificate signed by the provider setting out such facts as the provider considers would assist in explaining:
 - (i) the operation of those individual transmission services or individual message/call application services (as the case may be); or
 - (ii) the way in which the intercepted communications, intercepted messages, intercepted voice calls or intercepted video calls (as the case may be) were made available by the provider to the relevant agency or the Organisation (as the case may be).

Stored communications

- (3) If:
 - (a) an international production order is directed to a prescribed communications provider; and
 - (b) the provider is not an individual; and
 - (c) the order requires the provider to:
 - (i) make a copy of stored communications; and
 - (ii) make the copy available to a relevant agency or the Organisation; and
 - (d) the stored communications consist of:
 - (i) communications that a person has made using a transmission service; or
 - (ii) messages that a person has sent or received using a message/call application service; or
 - (iii) recordings of voice calls that a person has made or received using a message/call application service; or
 - (iv) recordings of video calls that a person has made or received using a message/call application service; or
 - (v) material that a person has uploaded for storage or back-up by a storage/back-up service; or

- (vi) material that a person has posted to a general electronic content service;
- a manager of the provider may do either or both of the following:
- (e) issue a written certificate signed by the manager setting out such facts as the manager considers relevant with respect to acts or things done by the provider in order to voluntarily give the relevant agency or the Organisation (as the case may be) in connection with the international production order, information relating to:
 - (i) those individual transmission services, those individual message/call application services, that storage/back-up service or that general electronic content service (as the case may be); or
 - (ii) the person;
 - (f) issue a written certificate signed by the manager setting out such facts as the manager considers would assist in explaining:
 - (i) the operation of those individual transmission services, those individual message/call application services, that storage/back-up service or that general electronic content service (as the case may be); or
 - (ii) the way in which the copy of the stored communications was made available by the provider to the relevant agency or the Organisation (as the case may be).
- (4) If:
- (a) an international production order is directed to a prescribed communications provider; and
 - (b) the provider is an individual; and
 - (c) the order requires the provider to:
 - (i) make a copy of stored communications; and
 - (ii) make the copy available to a relevant agency or the Organisation; and
 - (d) the stored communications consist of:
 - (i) communications that a person has made using a transmission service; or

Clause 162

- (ii) messages that a person has sent or received using a message/call application service; or
- (iii) recordings of voice calls that a person has made or received using a message/call application service; or
- (iv) recordings of video calls that a person has made or received using a message/call application service; or
- (v) material that a person has uploaded for storage or back-up by a storage/back-up service; or
- (vi) material that a person has posted to a general electronic content service;

the provider may do either or both of the following:

- (e) issue a written certificate signed by the provider setting out such facts as the provider considers relevant with respect to acts or things done by the provider in order to voluntarily give the relevant agency or the Organisation (as the case may be) in connection with the international production order, information relating to:
 - (i) those individual transmission services, those individual message/call application services, that storage/back-up service or that general electronic content service (as the case may be); or
 - (ii) the person;
- (f) issue a written certificate signed by the provider setting out such facts as the provider considers would assist in explaining:
 - (i) the operation of those individual transmission services, those individual message/call application services, that storage/back-up service or that general electronic content service (as the case may be); or
 - (ii) the way in which the copy of the stored communications was made available by the provider to the relevant agency or the Organisation (as the case may be).

Telecommunications data

(5) If:

- (a) an international production order is directed to a prescribed communications provider; and
 - (b) the provider is not an individual; and
 - (c) the order requires the provider to disclose to a relevant agency, or to the Organisation, telecommunications data that relates to:
 - (i) communications carried by an individual transmission service; or
 - (ii) an individual transmission service; or
 - (iii) messages sent or received using an individual message/call application service; or
 - (iv) voice calls made or received using an individual message/call application service; or
 - (v) video calls made or received using an individual message/call application service; or
 - (vi) an individual message/call application service; or
 - (vii) material that has been uploaded by an end-user for storage or back-up by a storage/back-up service; or
 - (viii) material that has been posted on a general electronic content service;
- a manager of the provider may do either or both of the following:
- (d) issue a written certificate signed by the manager setting out such facts as the manager considers relevant with respect to acts or things done by the provider in order to voluntarily give the relevant agency or the Organisation (as the case may be) in connection with the international production order, information relating to those individual transmission services, those individual message/call application services, that storage/back-up service or that general electronic content service (as the case may be);
 - (e) issue a written certificate signed by the manager setting out such facts as the manager considers would assist in explaining:
 - (i) the operation of those individual transmission services, those individual message/call application services, that

Clause 162

storage/back-up service or that general electronic content service (as the case may be); or

- (ii) the way in which the telecommunications data was disclosed by the provider to the relevant agency or the Organisation (as the case may be).

(6) If:

- (a) an international production order is directed to a prescribed communications provider; and
- (b) the provider is an individual; and
- (c) the order requires the provider to disclose to a relevant agency, or to the Organisation, telecommunications data that relates to:
 - (i) communications carried by an individual transmission service; or
 - (ii) an individual transmission service; or
 - (iii) messages sent or received using an individual message/call application service; or
 - (iv) voice calls made or received using an individual message/call application service; or
 - (v) video calls made or received using an individual message/call application service; or
 - (vi) an individual message/call application service; or
 - (vii) material that has been uploaded by an end-user for storage or back-up by a storage/back-up service; or
 - (viii) material that has been posted on a general electronic content service;

the provider may do either or both of the following:

- (d) issue a written certificate signed by the provider setting out such facts as the provider considers relevant with respect to acts or things done by the provider in order to voluntarily give the relevant agency or the Organisation (as the case may be) in connection with the international production order, information relating to those individual transmission services, those individual message/call application services,

- that storage/back-up service or that general electronic content service (as the case may be);
- (e) issue a written certificate signed by the provider setting out such facts as the provider considers would assist in explaining:
- (i) the operation of those individual transmission services, those individual message/call application services, that storage/back-up service or that general electronic content service (as the case may be); or
 - (ii) the way in which the telecommunications data was disclosed by the provider to the relevant agency or the Organisation (as the case may be).

Evidentiary effect

- (7) A document purporting to be a certificate issued under subclause (1), (2), (3), (4), (5) or (6) in connection with an international production order:
- (a) is to be received in evidence in a proceeding in Australia without further proof; and
 - (b) in a proceeding in Australia, is prima facie evidence of the matters stated in the document;
- so long as information obtained in accordance with the order is admissible in those proceedings.

163 Evidentiary certificates—interception

- (1) A certifying officer of an interception agency may issue a written certificate signed by the officer setting out such facts as the officer considers relevant with respect to:
- (a) the receipt by the agency of:
 - (i) intercepted communications; or
 - (ii) intercepted messages; or
 - (iii) intercepted voice calls; or
 - (iv) intercepted video calls;that were made available to the agency in accordance with an international production order issued under clause 30; or

Clause 163

- (b) the receipt by the agency of telecommunications data that was disclosed to the agency in accordance with an international production order issued under clause 30.
- (2) A certifying officer of a Part 5.3 IPO agency may issue a written certificate signed by the officer setting out such facts as the officer considers relevant with respect to:
 - (a) the receipt by the agency of:
 - (i) intercepted communications; or
 - (ii) intercepted messages; or
 - (iii) intercepted voice calls; or
 - (iv) intercepted video calls;that were made available to the agency in accordance with an international production order issued under clause 60; or
 - (b) the receipt by the agency of telecommunications data that was disclosed to the agency in accordance with an international production order issued under clause 60.
- (3) A certifying person may issue a written certificate signed by the person setting out such facts as the person considers relevant with respect to:
 - (a) the receipt by the Organisation of:
 - (i) intercepted communications; or
 - (ii) intercepted messages; or
 - (iii) intercepted voice calls; or
 - (iv) intercepted video calls;that were made available to the Organisation in accordance with an international production order issued under clause 89; or
 - (b) the receipt by the Organisation of telecommunications data that was disclosed to the Organisation in accordance with an international production order issued under clause 89.
- (4) A document purporting to be a certificate issued under subclause (1), (2) or (3):

- (a) is to be received in evidence in a proceeding in Australia without further proof; and
- (b) in a proceeding in Australia, is prima facie evidence of the matters stated in the document.

164 Evidentiary certificates—stored communications

- (1) A certifying officer of a criminal law-enforcement agency may issue a written certificate signed by the officer setting out such facts as the officer considers relevant with respect to:
 - (a) the receipt by the agency of a copy of stored communications that were made available to the agency in accordance with an international production order issued under clause 39; or
 - (b) the receipt by the agency of telecommunications data that was disclosed to the agency in accordance with an international production order issued under clause 39.
- (2) A certifying officer of a Part 5.3 IPO agency may issue a written certificate signed by the officer setting out such facts as the officer considers relevant with respect to:
 - (a) the receipt by the agency of a copy of stored communications that were made available to the agency in accordance with an international production order issued under clause 69; or
 - (b) the receipt by the agency of telecommunications data that was disclosed to the agency in accordance with an international production order issued under clause 69.
- (3) A certifying person may issue a written certificate signed by the person setting out such facts as the person considers relevant with respect to:
 - (a) the receipt by the Organisation of a copy of stored communications that were made available to the Organisation in accordance with an international production order issued under clause 98; or
 - (b) the receipt by the Organisation of telecommunications data that was disclosed to the Organisation in accordance with an international production order issued under clause 98.

Clause 165

- (4) A document purporting to be a certificate issued under subclause (1), (2) or (3):
 - (a) is to be received in evidence in a proceeding in Australia without further proof; and
 - (b) in a proceeding in Australia, is prima facie evidence of the matters stated in the document.

165 Evidentiary certificates—telecommunications data

- (1) A certifying officer of an enforcement agency may issue a written certificate signed by the officer setting out such facts as the officer considers relevant with respect to the receipt by the agency of telecommunications data that was disclosed to the agency in accordance with an international production order issued under clause 48.
- (2) A certifying officer of a Part 5.3 IPO agency may issue a written certificate signed by the officer setting out such facts as the officer considers relevant with respect to the receipt by the agency of telecommunications data that was disclosed to the agency in accordance with an international production order issued under clause 78.
- (3) A certifying person may issue a written certificate signed by the person setting out such facts as the person considers relevant with respect to the receipt by the Organisation of telecommunications data that was disclosed to the Organisation in accordance with an international production order issued under clause 107.
- (4) A document purporting to be a certificate issued under subclause (1), (2) or (3):
 - (a) is to be received in evidence in a proceeding in Australia without further proof; and
 - (b) in a proceeding in Australia, is prima facie evidence of the matters stated in the document.

166 Evidentiary certificates—Australian Designated Authority

- (1) The Australian Designated Authority may issue a written certificate signed by the Australian Designated Authority setting out such facts as the Australian Designated Authority considers relevant with respect to:
 - (a) giving an international production order to a prescribed communications provider; or
 - (b) giving an instrument of revocation of an international production order to a prescribed communications provider; or
 - (c) giving an instrument of cancellation to a prescribed communications provider.

- (2) If an international production order requires a prescribed communications provider to make intercepted communications, intercepted messages, intercepted voice calls or intercepted video calls available to:
 - (a) an interception agency; or
 - (b) a Part 5.3 IPO agency; or
 - (c) the Organisation;
indirectly via the Australian Designated Authority, the Australian Designated Authority may issue a written certificate signed by the Australian Designated Authority setting out such facts as the Australian Designated Authority considers relevant with respect to:
 - (d) the receipt by the Australian Designated Authority of the intercepted communications, intercepted messages, intercepted voice calls or intercepted video calls; or
 - (e) anything done by the Australian Designated Authority for the purposes of ensuring that the intercepted communications, intercepted messages, intercepted voice calls or intercepted video calls were passed on to the agency or Organisation, as the case requires.

- (3) If an international production order requires a prescribed communications provider to make a copy of stored communications available to:
 - (a) a criminal law-enforcement agency; or

Clause 166

- (b) a Part 5.3 IPO agency; or
 - (c) the Organisation;indirectly via the Australian Designated Authority, the Australian Designated Authority may issue a written certificate signed by the Australian Designated Authority setting out such facts as the Australian Designated Authority considers relevant with respect to:
 - (d) the receipt by the Australian Designated Authority of the copy; or
 - (e) anything done by the Australian Designated Authority for the purposes of ensuring that the copy was passed on to the agency or Organisation, as the case requires.
- (4) If an international production order requires a prescribed communications provider to disclose telecommunications data to:
 - (a) a relevant agency; or
 - (b) the Organisation;indirectly via the Australian Designated Authority, the Australian Designated Authority may issue a written certificate signed by the Australian Designated Authority setting out such facts as the Australian Designated Authority considers relevant with respect to:
 - (c) the receipt by the Australian Designated Authority of the telecommunications data; or
 - (d) anything done by the Australian Designated Authority for the purposes of ensuring that the telecommunications data was passed on to the agency or Organisation, as the case requires.
- (5) A document purporting to be a certificate issued under subclause (1), (2), (3) or (4):
 - (a) is to be received in evidence in a proceeding in Australia without further proof; and
 - (b) in a proceeding in Australia, is prima facie evidence of the matters stated in the document.

Part 13—Incoming orders and requests

167 Simplified outline of this Part

- If there is a designated international agreement between Australia and one or more foreign countries, and a competent authority of such a foreign country issues an order, or makes a request, covered by the agreement, an act or thing done in compliance with such an order or request is exempt from:
 - (a) the provisions of this Act that prohibit intercepting communications and accessing stored communications; and
 - (b) the provisions of this Act that prohibit disclosure of information; and
 - (c) the provisions of the *Telecommunications Act 1997* that prohibit the disclosure of information.

168 Incoming orders and requests—exemptions from various prohibitions

If:

- (a) there is a designated international agreement between Australia and one or more foreign countries; and
- (b) the agreement deals with (among other things):
 - (i) the issue of orders (however described); or
 - (ii) the making of requests (however described);by a competent authority (however described) of such a foreign country;

then:

- (c) subsections 7(1) and 108(1) do not apply to or in relation to:
 - (i) an act or thing done in compliance with such an order or request; or

Clause 169

- (ii) the issue of such an order or the making of such a request; and
- (d) subsections 63(1) and 133(1) do not apply to or in relation to:
 - (i) an act or thing done in compliance with such an order or request; or
 - (ii) information obtained in accordance with such an order or request; and
- (e) sections 276, 277 and 278 of the *Telecommunications Act 1997* do not apply to or in relation to:
 - (i) an act or thing done in compliance with such an order or request; or
 - (ii) information obtained in accordance with such an order or request.

- Note 1: In a prosecution for an offence against subsection 7(1) or 108(1), a defendant bears an evidential burden in relation to the matter in paragraph (c): see subsection 13.3(3) of the *Criminal Code*.
- Note 2: In a prosecution for an offence against subsection 63(1) or 133(1), a defendant bears an evidential burden in relation to the matter in paragraph (d): see subsection 13.3(3) of the *Criminal Code*.
- Note 3: In a prosecution for an offence against section 276, 277 or 278 of the *Telecommunications Act 1997*, a defendant bears an evidential burden in relation to the matter in paragraph (e): see subsection 13.3(3) of the *Criminal Code*.

169 Interaction with the *Privacy Act 1988*

For the purposes of the *Privacy Act 1988*, if:

- (a) there is a designated international agreement between Australia and one or more foreign countries; and
- (b) the agreement deals with (among other things):
 - (i) the issue of orders (however described); or
 - (ii) the making of requests (however described);by a competent authority (however described) of such a foreign country;

the disclosure of information in compliance with any such order or request, to the extent that the information contains personal

information, is taken to be a disclosure that is authorised by this Act.

Part 14—Miscellaneous

170 Simplified outline of this Part

- This Part deals with miscellaneous matters, such as:
 - (a) electronic service of documents; and
 - (b) certified copies of international production orders; and
 - (c) delegations.

171 Electronic service of documents

(1) If:

- (a) any of the following is required by this Schedule to be given to a person by the Australian Designated Authority:
 - (i) an international production order;
 - (ii) a certified copy of an international production order;
 - (iii) an instrument of revocation of an international production order;
 - (iv) an instrument of cancellation of an international production order; and
- (b) the person has nominated an electronic address for service in a document given by the person to the Australian Designated Authority;

the order, copy or instrument is taken to have been given to the person if it is sent to the nominated electronic address for service.

(2) If:

- (a) any of the following is required by this Schedule to be given to the Australian Designated Authority by a person, a relevant agency or the Organisation:
 - (i) an international production order;
 - (ii) a certified copy of an international production order;

- (iii) an instrument of revocation of an international production order;
 - (iv) an instrument of cancellation of an international production order; and
 - (b) the Australian Designated Authority has nominated an electronic address for service in a document given by the Australian Designated Authority to the person, the relevant agency or the Organisation, as the case may be;
- the order, copy or instrument is taken to have been given to the Australian Designated Authority if it is sent to the nominated electronic address for service.

172 International production order issued in response to a telephone application—action required

Scope

- (1) This clause applies if a person (the *issuing person*) issues an international production order in response to a telephone application made by a person (the *applicant*) on behalf of:
 - (a) a relevant agency; or
 - (b) the Organisation.

Required action

- (2) Within one day after the day on which the international production order is issued, the applicant must:
 - (a) cause each person who gave information to the issuing person in connection with the application to swear or affirm an affidavit setting out the information so given by the person; and
 - (b) give to the issuing person:
 - (i) the affidavit or affidavits; and
 - (ii) if, as a result of an authorisation that was in force under clause 23, 34, 43, 53, 64 or 73 when the application was made, the applicant was authorised to make the application by telephone—a copy of the authorisation.

Clause 172

Cancellation if required action not taken

- (3) If the issuing person is satisfied that subclause (2) has not been complied with in relation to the order, the issuing person may cancel the order.
- (4) A cancellation under subclause (3) is to be set out in a written instrument.
- (5) If the international production order is cancelled by the issuing person under subclause (3):
 - (a) the issuing person must:
 - (i) give the instrument of cancellation to the Australian Designated Authority; and
 - (ii) do so as soon as practicable after the order is cancelled; and
 - (b) if the telephone application was made on behalf of a relevant agency—the Australian Designated Authority must:
 - (i) inform the chief officer of the relevant agency of the cancellation; and
 - (ii) do so as soon as practicable after the instrument of cancellation is given to the Australian Designated Authority; and
 - (c) if the telephone application was made on behalf of the Organisation—the Australian Designated Authority must:
 - (i) inform the Organisation of the cancellation; and
 - (ii) do so as soon as practicable after the instrument of cancellation is given to the Australian Designated Authority.
- (6) If:
 - (a) the Australian Designated Authority gave the international production order to the prescribed communications provider to whom the order is directed; and
 - (b) the order was subsequently cancelled under subclause (3);the Australian Designated Authority must:

- (c) give the instrument of cancellation to the prescribed communications provider; and
 - (d) do so as soon as practicable after the instrument of cancellation is given to the Australian Designated Authority.
- (7) A cancellation under subclause (3) takes effect:
- (a) if the instrument of cancellation is required to be given to the prescribed communications provider concerned—when the instrument is given; or
 - (b) otherwise—when the cancellation is made.
- (8) If:
- (a) an international production order is cancelled under this clause; and
 - (b) when the cancellation takes effect, the Australian Designated Authority has not made a decision about the order under clause 111 or 112 (as the case may be);
- clause 111 or 112 (as the case may be) ceases to apply to the order when the cancellation takes effect.

173 Duty of nominated AAT Security Division member

It is the duty of a nominated AAT Security Division member to ensure, so far as the member is able to do so, that, in or in connection with the performance of a function, or the exercise of a power, conferred on the member by this Schedule, information is not communicated or made available to a person contrary to the requirements of security (within the ordinary meaning of that expression).

174 Certified copy of international production order—interception agency

- (1) A document certified in writing by a certifying officer of an interception agency to be a true copy of an international production order issued under clause 30 is to be received in evidence in a proceeding mentioned in clause 153 or 157 as if it were the original international production order.

Clause 175

- (2) The document is to be known as a *certified copy* of the original international production order.

175 Certified copy of international production order—criminal law-enforcement agency

- (1) A document certified in writing by a certifying officer of a criminal law-enforcement agency to be a true copy of an international production order issued under clause 39 is to be received in evidence in a proceeding mentioned in clause 153 or 158 as if it were the original international production order.
- (2) The document is to be known as a *certified copy* of the original international production order.

176 Certified copy of international production order—enforcement agency

- (1) A document certified in writing by a certifying officer of an enforcement agency to be a true copy of an international production order issued under clause 48 is to be received in evidence in:
- (a) a proceeding mentioned in clause 153; or
 - (b) a proceeding for a purpose mentioned in clause 159;
- as if it were the original international production order.
- (2) The document is to be known as a *certified copy* of the original international production order.

177 Certified copy of international production order—Part 5.3 IPO agency

Interception

- (1) A document certified in writing by a certifying officer of a Part 5.3 IPO agency to be a true copy of an international production order issued under clause 60 is to be received in evidence in:
- (a) a proceeding by way of a prosecution for an offence against:

- (i) Part 5.3 of the *Criminal Code*; or
 - (ii) Part 5.5 of the *Criminal Code*; or
 - (b) a proceeding mentioned in clause 153; or
 - (c) a proceeding mentioned in clause 157;
- as if it were the original international production order.
- (2) The document is to be known as a ***certified copy*** of the original international production order.

Stored communications

- (3) A document certified in writing by a certifying officer of a Part 5.3 IPO agency to be a true copy of an international production order issued under clause 69 is to be received in evidence in:
- (a) a proceeding by way of a prosecution for an offence against:
 - (i) Part 5.3 of the *Criminal Code*; or
 - (ii) Part 5.5 of the *Criminal Code*; or
 - (b) a proceeding mentioned in clause 153; or
 - (c) a proceeding mentioned in clause 158;
- as if it were the original international production order.
- (4) The document is to be known as a ***certified copy*** of the original international production order.

Telecommunications data

- (5) A document certified in writing by a certifying officer of a Part 5.3 IPO agency to be a true copy of an international production order issued under clause 78 is to be received in evidence in:
- (a) a proceeding by way of a prosecution for an offence against:
 - (i) Part 5.3 of the *Criminal Code*; or
 - (ii) Part 5.5 of the *Criminal Code*; or
 - (b) a proceeding mentioned in clause 153; or
 - (c) a proceeding for a purpose mentioned in clause 159;
- as if it were the original international production order.

Clause 178

- (6) The document is to be known as a *certified copy* of the original international production order.

178 Certified copy of international production order—the Organisation

Interception

- (1) A document certified in writing by a certifying person to be a true copy of an international production order issued under clause 89 is to be received in evidence in a proceeding mentioned in clause 153 or 157 as if it were the original international production order.
- (2) The document is to be known as a *certified copy* of the original international production order.

Stored communications

- (3) A document certified in writing by a certifying person to be a true copy of an international production order issued under clause 98 is to be received in evidence in a proceeding mentioned in clause 153 or 158 as if it were the original international production order.
- (4) The document is to be known as a *certified copy* of the original international production order.

Telecommunications data

- (5) A document certified in writing by a certifying person to be a true copy of an international production order issued under clause 107 is to be received in evidence in:
- (a) a proceeding mentioned in clause 153; or
 - (b) a proceeding for a purpose mentioned in clause 159;
- as if it were the original international production order.
- (6) The document is to be known as a *certified copy* of the original international production order.

179 Delegation by the Australian Designated Authority

- (1) The Australian Designated Authority may, by writing, delegate any or all of the Australian Designated Authority's functions or powers under this Schedule to:
- (a) an SES employee, or acting SES employee, in the Attorney-General's Department; or
 - (b) an APS employee who holds, or is acting in, an Executive Level 1 or 2 position in the Attorney-General's Department.

Note: The expressions *SES employee*, *acting SES employee* and *APS employee* are defined in section 2B of the *Acts Interpretation Act 1901*.

- (2) In performing functions, or exercising powers, under a delegation under subclause (1), the delegate must comply with any directions of the Australian Designated Authority.

180 Minor defects in connection with international production order

- (1) If:
- (a) information is purportedly obtained in accordance with an international production order; and
 - (b) there is a defect or irregularity in relation to the international production order; and
 - (c) apart from that defect or irregularity, the information would have been obtained in accordance with the international production order;
- the information is taken to have been obtained in accordance with the international production order.
- (2) For the purposes of subclause (1), a ***defect or irregularity*** in relation to an international production order means a defect or irregularity:
- (a) that is not a substantial defect or irregularity; and
 - (b) that is:
 - (i) in, or in connection with the issue of, a document purporting to be the international production order; or

Clause 181

- (ii) in connection with compliance with the international production order; or
- (iii) in connection with purported compliance with a document purporting to be the international production order.

181 Protection of persons—control order declared to be void

- (1) If:
 - (a) an international production order was issued under Part 3 of this Schedule on the basis that an interim control order was in force; and
 - (b) a court subsequently declares the interim control order to be void;a criminal proceeding does not lie against a person in respect of anything done in good faith by the person in purported compliance with the international production order.
- (2) Subclause (1) does not apply to a thing done at a particular time if, at that time, the person knew, or ought reasonably to have known, of the declaration.

182 Specification of international agreements

- (1) If:
 - (a) there is an agreement between Australia and one or more foreign countries; and
 - (b) the name of the agreement is specified in:
 - (i) regulations made for the purposes of this Schedule; or
 - (ii) an application made under this Schedule; or
 - (iii) an international production order; or
 - (iv) any other instrument made under this Schedule;a reference in the regulations, application, order or other instrument (as the case may be) to the agreement is a reference to the agreement as amended and in force for Australia from time to time.

- (2) For the purposes of subclause (1), disregard an amendment of an agreement unless:
- (a) a copy of the English text of the amendment is set out in regulations made for the purposes of paragraph 3(1)(d) or (3)(d); and
 - (b) the amendment has entered into force for Australia.

183 Operation of the *Mutual Assistance in Criminal Matters Act 1987* not limited

This Schedule is not intended to limit the operation of the *Mutual Assistance in Criminal Matters Act 1987*.

184 Other functions or powers not limited

This Schedule is not intended to limit the functions or powers of:

- (a) a relevant agency; or
 - (b) the Organisation; or
 - (c) any other body or person;
- to request or obtain assistance or information from:
- (d) a prescribed communications provider; or
 - (e) any other body or person.

Endnotes

Endnote 1—About the endnotes

Endnotes

Endnote 1—About the endnotes

The endnotes provide information about this compilation and the compiled law.

The following endnotes are included in every compilation:

Endnote 1—About the endnotes

Endnote 2—Abbreviation key

Endnote 3—Legislation history

Endnote 4—Amendment history

Abbreviation key—Endnote 2

The abbreviation key sets out abbreviations that may be used in the endnotes.

Legislation history and amendment history—Endnotes 3 and 4

Amending laws are annotated in the legislation history and amendment history.

The legislation history in endnote 3 provides information about each law that has amended (or will amend) the compiled law. The information includes commencement details for amending laws and details of any application, saving or transitional provisions that are not included in this compilation.

The amendment history in endnote 4 provides information about amendments at the provision (generally section or equivalent) level. It also includes information about any provision of the compiled law that has been repealed in accordance with a provision of the law.

Editorial changes

The *Legislation Act 2003* authorises First Parliamentary Counsel to make editorial and presentational changes to a compiled law in preparing a compilation of the law for registration. The changes must not change the effect of the law. Editorial changes take effect from the compilation registration date.

If the compilation includes editorial changes, the endnotes include a brief outline of the changes in general terms. Full details of any changes can be obtained from the Office of Parliamentary Counsel.

Misdescribed amendments

A misdescribed amendment is an amendment that does not accurately describe the amendment to be made. If, despite the misdescription, the amendment can

Endnote 1—About the endnotes

be given effect as intended, the amendment is incorporated into the compiled law and the abbreviation “(md)” added to the details of the amendment included in the amendment history.

If a misdescribed amendment cannot be given effect as intended, the abbreviation “(md not incorp)” is added to the details of the amendment included in the amendment history.

Endnotes

Endnote 2—Abbreviation key

Endnote 2—Abbreviation key

ad = added or inserted	o = order(s)
am = amended	Ord = Ordinance
amdt = amendment	orig = original
c = clause(s)	par = paragraph(s)/subparagraph(s) /sub-subparagraph(s)
C[x] = Compilation No. x	pres = present
Ch = Chapter(s)	prev = previous
def = definition(s)	(prev...) = previously
Dict = Dictionary	Pt = Part(s)
disallowed = disallowed by Parliament	r = regulation(s)/rule(s)
Div = Division(s)	reloc = relocated
ed = editorial change	renum = renumbered
exp = expires/expired or ceases/ceased to have effect	rep = repealed
F = Federal Register of Legislation	rs = repealed and substituted
gaz = gazette	s = section(s)/subsection(s)
LA = <i>Legislation Act 2003</i>	Sch = Schedule(s)
LIA = <i>Legislative Instruments Act 2003</i>	Sdiv = Subdivision(s)
(md) = misdescribed amendment can be given effect	SLI = Select Legislative Instrument
(md not incorp) = misdescribed amendment cannot be given effect	SR = Statutory Rules
mod = modified/modification	Sub-Ch = Sub-Chapter(s)
No. = Number(s)	SubPt = Subpart(s)
	<u>underlining</u> = whole or part not commenced or to be commenced

Endnote 3—Legislation history

Endnote 3—Legislation history

Act	Number and year	Assent	Commencement	Application, saving and transitional provisions
Telecommunications (Interception) Act 1979	114, 1979	25 Oct 1979	1 June 1980 (<i>see Gazette</i> 1980, No. G21, p. 2)	—
Telecommunications (Interception) Amendment Act 1979	181, 1979	4 Dec 1979	1 June 1980 (<i>see s. 2 and Gazette</i> 1980, No. G21, p. 2)	—
Director of Public Prosecutions (Consequential Amendments) Act 1983	114, 1983	14 Dec 1983	s. 8(1): 16 Dec 1985 (<i>see s. 2(2)</i>) s. 8(2): 16 Dec 1985 (<i>see s. 2(3)</i>) Remainder: 5 Mar 1984 (<i>see s. 2(1) and Gazette</i> 1984, No. S55)	—
Telecommunications (Interception) Amendment Act 1983	116, 1983	16 Dec 1983	16 Dec 1983	—
Telecommunications (Interception) Amendment Act 1984	6, 1984	4 Apr 1984	4 Apr 1984	s 4
Telecommunications (Interception) Amendment Act (No. 2) 1984	116, 1984	17 Oct 1984	17 Oct 1984	—
Telecommunications (Interception) Amendment Act 1985	8, 1985	29 Mar 1985	29 Mar 1985	—
Telecommunications (Interception) Amendment Act (No. 2) 1985	63, 1985	4 June 1985	4 June 1985	ss. 2(2) and 8

Telecommunications (Interception and Access) Act 1979

669

Compilation No. 117

Compilation date: 02/04/2022

Registered: 26/04/2022

Endnotes

Endnote 3—Legislation history

Act	Number and year	Assent	Commencement	Application, saving and transitional provisions
Intelligence and Security (Consequential Amendments) Act 1986	102, 1986	17 Oct 1986	s 25–34: 1 Feb 1987 (s 2)	—
as amended by				
Crimes Legislation Amendment Act 1991	28, 1991	4 Mar 1991	Sch 2 (Pt 3): 1 Feb 1987 (s 2(7))	—
Telecommunications (Interception) Amendment Act 1987	89, 1987	5 June 1987	s 3, 4, 5(1)(b), 7, 9–21 and Sch 1: 1 Sept 1988 (s 2(2) and gaz 1988, No S256) s 5(1)(a), (2), 6 and 8: 16 Dec 1987 (s 2(1A))	s 6(2), 16(2), (3), 17(2) and 18(2)–(4)
as amended by				
Crimes Legislation Amendment Act 1987	120, 1987	16 Dec 1987	s 54: 16 Dec 1987 (s 2(3))	—
Crimes Legislation Amendment Act 1987	120, 1987	16 Dec 1987	s 56–59: 16 Dec 1987 (s 2(3) and (4)) s 60–67: 1 Sept 1988 (s 2(5))	—
Extradition (Repeal and Consequential Provisions) Act 1988	5, 1988	9 Mar 1988	s 7(2), (3) and Sch: 1 Dec 1988 (s 2(1) and (3)(a))	s 7(2) and (3)
Crimes Legislation Amendment Act 1988	65, 1988	15 June 1988	ss. 9–11: 1 Sept 1988 (see s. 2(2), (3) and <i>Gazette</i> 1988, No. S256) Remainder: Royal Assent	—
Crimes Legislation Amendment Act (No. 2) 1988	66, 1988	15 June 1988	s 26–28: 1 Sept 1988 (s 2(5))	—

Endnote 3—Legislation history

Act	Number and year	Assent	Commencement	Application, saving and transitional provisions
Statutory Instruments (Tabling and Disallowance) Legislation Amendment Act 1988	99, 1988	2 Dec 1988	2 Dec 1988	—
Telecommunications Amendment Act 1988	121, 1988	14 Dec 1988	ss. 5, 6, 10, 12, 13, 23(2) and 26(1): 1 Jan 1989 (see <i>Gazette</i> 1988, No. S402) ss. 14, 23(3) and 26(2): 30 June 1989 (see <i>Gazette</i> 1989, No. S216) Remainder: Royal Assent	—
Telecommunications and Postal Services (Transitional Provisions and Consequential Amendments) Act 1989	63, 1989	19 June 1989	s 38–59: 1 July 1989 (s 2(1) and gaz 1989, No S230)	—
as amended by Transport and Communications Legislation Amendment Act 1990	11, 1991	21 Jan 1991	Sch: 1 July 1989 (s 2(13)(e))	—
Law and Justice Legislation Amendment Act 1989	11, 1990	17 Jan 1990	s 51(1)(a), 52–55 and Sch 2: 14 Feb 1990 (s 2(1)) s 51(1)(b) and (2): 17 Jan 1990 (s 2(5)(b))	s 51(2)
Crimes Legislation Amendment Act 1991	28, 1991	4 Mar 1991	s 61(1), 64–66 and 68–72: 4 Mar 1991 (s 2(1)) s 61(2), 62, 63, 67 and 73: 29 Apr 1991 (s 2(2) and gaz 1991, No S108)	s 73

Telecommunications (Interception and Access) Act 1979

671

Compilation No. 117

Compilation date: 02/04/2022

Registered: 26/04/2022

Endnotes

Endnote 3—Legislation history

Act	Number and year	Assent	Commencement	Application, saving and transitional provisions
Telecommunications (Transitional Provisions and Consequential Amendments) Act 1991	99, 1991	27 June 1991	ss. 1 and 2: Royal Assent ss. 3–23 and 25: 1 July 1991 Remainder: 1 Feb 1992 (see s. 2(3) and <i>Gazette</i> 1992, No. S32)	—
Telecommunications (Interception) Amendment Act 1993	103, 1993	22 Dec 1993	ss. 3(2), 5, 12, 14–18 and 24–28: 1 Feb 1994 (see <i>Gazette</i> 1994, No. S27) Remainder: Royal Assent	s 3(3), 17(2), (3), 24(2) and 25(2), (3)
Royal Commission into the New South Wales Police Service (Access to Information) Act 1994	170, 1994	16 Dec 1994	16 Dec 1994	—
Evidence (Transitional Provisions and Consequential Amendments) Act 1995	3, 1995	23 Feb 1995	s 14: 23 Feb 1995 (s 2(1)) Sch: 18 Apr 1995 (s 2(13)(a))	s 14
International War Crimes Tribunals (Consequential Amendments) Act 1995	19, 1995	29 Mar 1995	s. 3: 28 Aug 1995 (see <i>Gazette</i> 1995, No. S323) Remainder: Royal Assent	—
Telecommunications (Interception) Amendment Act 1995	141, 1995	12 Dec 1995	Schedule 1 (Part 2): 12 June 1996 Remainder: Royal Assent	Sch 1 (items 3, 14, 19, 34, 36, 39)
Statute Law Revision Act 1996	43, 1996	25 Oct 1996	Sch 5 (items 147–149): 25 Oct 1996 (s 2(1))	—
Telecommunications (Transitional Provisions and Consequential Amendments) Act 1997	59, 1997	3 May 1997	Sch 1 (items 51–55): 1 July 1997 (s 2(2)(d))	—

Endnote 3—Legislation history

Act	Number and year	Assent	Commencement	Application, saving and transitional provisions
Telecommunications (Interception) and Listening Device Amendment Act 1997	160, 1997	11 Nov 1997	Schedule 1 (items 6, 19, 20, 24, 25, 27–39, 47–50), Schedule 2 and Schedule 3 (items 1–8, 11–13): 1 Feb 1998 (<i>see Gazette</i> 1998, No. GN3) Remainder: Royal Assent	s 3 (rep. by 151, 1999, Sch. 2)
as amended by				
Telecommunications (Interception) Amendment Act 1999	151, 1999	11 Nov 1999	11 Nov 1999	—
Migration Legislation Amendment Act (No. 1) 1999	89, 1999	16 July 1999	Sch 2: 22 July 1999 (s 2(4) and gaz 1999, No S337)	—
Public Employment (Consequential and Transitional) Amendment Act 1999	146, 1999	11 Nov 1999	Sch 1 (item 918): 5 Dec 1999 (s 2(1) and (2))	—
Telecommunications (Interception) Amendment Act 1999	151, 1999	11 Nov 1999	11 Nov 1999	—
Australian Security Intelligence Organisation Legislation Amendment Act 1999	161, 1999	10 Dec 1999	Sch 3 (items 1, 62–81): 10 Dec 1999 (s 2(2))	—
Australian Federal Police Legislation Amendment Act 2000	9, 2000	7 Mar 2000	Sch 2 (items 58–64) and Sch 3 (items 20, 32, 34, 35): 2 July 2000 (s 2(1) and gaz 2000, No S328)	Sch 3 (items 20, 32, 34, 35)

Telecommunications (Interception and Access) Act 1979

673

Compilation No. 117

Compilation date: 02/04/2022

Registered: 26/04/2022

Endnotes

Endnote 3—Legislation history

Act	Number and year	Assent	Commencement	Application, saving and transitional provisions
Telecommunications (Interception) Legislation Amendment Act 2000	63, 2000	22 June 2000	Sch 1, 2 and Sch 3 (items 4–72): 22 June 2000 (s 2(1)) Sch 3 (items 2, 3): 2 July 2000 (s 2(2))	Sch 3 (item 72)
Criminal Code Amendment (Theft, Fraud, Bribery and Related Offences) Act 2000	137, 2000	24 Nov 2000	Sch 2 (items 399, 400, 418, 419): 24 May 2001 (s 2(3))	Sch 2 (items 418, 419)
Law and Justice Legislation Amendment (Application of Criminal Code) Act 2001	24, 2001	6 Apr 2001	s 4(1), (2) and Sch 47: 24 May 2001 (s 2(1)(a))	s 4(1) and (2)
Corporations (Repeals, Consequential and Transitionals) Act 2001	55, 2001	28 June 2001	s 4–14 and Sch 3 (items 513–515): 15 July 2001 (s 2(1), (3))	s 4–14
National Crime Authority Legislation Amendment Act 2001	135, 2001	1 Oct 2001	Sch 1–7 and 9–12: 12 Oct 2001 (<i>see Gazette</i> 2001, No. S428) Sch 8: 13 Oct 2001 (<i>see Gazette</i> 2001, No. S428) Remainder: Royal Assent	—

Endnote 3—Legislation history

Act	Number and year	Assent	Commencement	Application, saving and transitional provisions
Cybercrime Act 2001	161, 2001	1 Oct 2001	21 Dec 2001 (<i>see Gazette</i> 2001, No. S529)	—
as amended by				
Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Act (No. 2) 2004	127, 2004	31 Aug 2004	(<i>see</i> 127, 2004 below)	—
Royal Commissions and Other Legislation Amendment Act 2001	166, 2001	1 Oct 2001	1 Oct 2001	—
International Criminal Court (Consequential Amendments) Act 2002	42, 2002	27 June 2002	Schedules 1–7: 26 Sept 2002 (<i>see</i> s. 2(1) and <i>Gazette</i> 2002, No. GN38) Remainder: 28 June 2002	—
Telecommunications Interception Legislation Amendment Act 2002	67, 2002	5 July 2002	Schedule 1 (items 23, 29, 33, 37, 39): 22 June 2000 Remainder: Royal Assent	Sch 2 (item 46)
Proceeds of Crime (Consequential Amendments and Transitional Provisions) Act 2002	86, 2002	11 Oct 2002	ss. 1–3: Royal Assent Remainder: 1 Jan 2003 (<i>see</i> s. 2(1) and <i>Gazette</i> 2002, No. GN44)	—
Australian Crime Commission Establishment Act 2002	125, 2002	10 Dec 2002	Sch 2 (items 190–224) and Sch 3 (item 17): 1 Jan 2003 (s 2(1) items 6, 10)	—

Telecommunications (Interception and Access) Act 1979

675

Compilation No. 117

Compilation date: 02/04/2022

Registered: 26/04/2022

Endnotes

Endnote 3—Legislation history

Act	Number and year	Assent	Commencement	Application, saving and transitional provisions
Australian Security Intelligence Organisation Legislation Amendment (Terrorism) Act 2003	77, 2003	22 July 2003	Schedule 1 (items 28, 29): 23 July 2003	Sch 1 (item 29)
Telecommunications Interception and Other Legislation Amendment Act 2003	113, 2003	12 Nov 2003	Schedule 1: 6 Feb 2004 (see <i>Gazette</i> 2004, No. S27) Remainder: Royal Assent	—
Telecommunications (Interception) Amendment Act 2004	55, 2004	27 Apr 2004	28 Apr 2004	—
Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Act (No. 2) 2004	127, 2004	31 Aug 2004	Sch 1 (items 25–31): 1 Mar 2005 (s 2(1) item 2)	Sch 1 (items 30, 31)
as amended by Telecommunications (Interception) Amendment Act 2006	40, 2006	3 May 2006	Sch 1 (item 16): 13 June 2006 (s 2(1) item 2)	—
Telecommunications (Interception) Amendment (Stored Communications) Act 2004	148, 2004	14 Dec 2004	15 Dec 2004	—

Endnote 3—Legislation history

Act	Number and year	Assent	Commencement	Application, saving and transitional provisions
Crimes Legislation Amendment (Telecommunications Interception and Other Measures) Act 2005	95, 2005	6 July 2005	Sch 2 (items 1, 2, 9): 17 Dec 2005 (s 2(1) items 3, 8) Sch 2 (items 3, 8, 10–14A): 6 July 2005 (s 2(1) items 4, 7, 9) Sch 2 (items 4, 5): never commenced (s 2(1) items 5, 6) Sch 2 (item 15): 1 June 1980 (s 2(1) item 10)	—
Criminal Code Amendment (Trafficking in Persons Offences) Act 2005	96, 2005	6 July 2005	Schedules 1 and 2: 3 Aug 2005 Remainder: Royal Assent	—
Statute Law Revision Act 2005	100, 2005	6 July 2005	Schedule 1 (items 66–82): Royal Assent	—
Intelligence Services Legislation Amendment Act 2005	128, 2005	4 Nov 2005	Sch 1–8: 2 Dec 2005 Remainder: Royal Assent	—
Law and Justice Legislation Amendment (Serious Drug Offences and Other Measures) Act 2005	129, 2005	8 Nov 2005	Schedule 1 (items 70–76): 6 Dec 2005	Sch 1 (items 75, 76)
Telecommunications (Interception) Amendment (Stored Communications and Other Measures) Act 2005	152, 2005	14 Dec 2005	Schedule 1 (items 3–18): 1 Oct 2006 (<i>see</i> F2006L03104) Remainder: Royal Assent	—

Telecommunications (Interception and Access) Act 1979

677

Compilation No. 117

Compilation date: 02/04/2022

Registered: 26/04/2022

Endnotes

Endnote 3—Legislation history

Act	Number and year	Assent	Commencement	Application, saving and transitional provisions
Telecommunications (Interception) Amendment Act 2006	40, 2006	3 May 2006	Sch 1 (items 1–9, 25–145), Sch 2 and Sch 3: 13 June 2006 (s 2(1) item 2) Sch 4: 1 July 2006 (s 2(1) item 3) Sch 5: 3 Nov 2006 (s 2(1) item 4) Sch 6 (items 1, 3): 1 Oct 2006 (s 2(1) items 5, 7) Sch 6 (items 2, 4–7, 9, 10): 3 May 2006 (s 2(1) items 6, 8, 10) Sch 6 (item 8): 1 Feb 1994 (s 2(1) item 9)	Sch 3 (items 6, 10), Sch 4 (items 31–34) and Sch 5 (items 19, 25, 29, 34)
as amended by				
Statute Law Revision Act 2007	8, 2007	15 Mar 2007	Sch 2 (item 15): 3 Nov 2006 (s 2(1) item 40)	—
Telecommunications (Interception and Access) Amendment Act 2007	177, 2007	28 Sept 2007	Sch 2 (item 1): 3 Nov 2006 (s 2(1) item 3)	—
Law Enforcement Integrity Commissioner (Consequential Amendments) Act 2006	86, 2006	30 June 2006	Sch 1 (items 76–85, 88–92): 30 Dec 2006 (s 2(1) items 2, 5) Sch 1 (items 86, 93–95): never commenced (s 2(1) item 3, 6) Sch 1 (items 87): 1 July 2006 (s 2(1) item 4) Sch 1 (item 96): 13 June 2006 (s 2(1) item 7)	—

Endnote 3—Legislation history

Act	Number and year	Assent	Commencement	Application, saving and transitional provisions
Law and Justice Legislation Amendment (Marking of Plastic Explosives) Act 2007	3, 2007	19 Feb 2007	Schedules 1–3: 25 Aug 2007 Remainder: Royal Assent	—
Telecommunications (Interception and Access) Amendment Act 2007	177, 2007	28 Sept 2007	Sch 1 (items 1–12, 55–68): 1 Nov 2007 (s 2(1) item 2) Sch 2 (items 2–26): 29 Sept 2007 (s 2(1) item 4)	Sch 1 (items 57–68) and Sch 2 (items 22–26)
Telecommunications (Interception and Access) Amendment Act 2008	23, 2008	26 May 2008	Schedule 1 (items 1–19): 27 May 2008 Schedule 1 (items 20–25, 35, 37, 39A): 1 July 2008 (see F2008L02096) Schedule 1 (items 43A, 46A): 1 July 2008 Remainder: Royal Assent	—
Telecommunications Interception Legislation Amendment Act 2008	95, 2008	3 Oct 2008	Sch 2 (items 1–11, 13, 21, 25–27): 4 Oct 2008 (s 2(1) items 3, 5, 7, 10) Sch 2 (items 12, 14–20, 22): 5 Dec 2008 (s 2(1) items 4, 6, 8) Sch 2 (items 23, 24): 3 Oct 2008 (s 2(1) item 9)	Sch 2 (items 25–27)
Telecommunications Interception Legislation Amendment Act (No. 1) 2009	32, 2009	22 May 2009	Schedule 1: 18 June 2009 (see s. 2(1)) Schedule 2 (items 2–4): 23 May 2009	Sch 2 (item 4)
Trade Practices Amendment (Cartel Conduct and Other Measures) Act 2009	59, 2009	26 June 2009	Schedule 1 (item 2): 24 July 2009	—

Telecommunications (Interception and Access) Act 1979

679

Compilation No. 117

Compilation date: 02/04/2022

Registered: 26/04/2022

Endnotes

Endnote 3—Legislation history

Act	Number and year	Assent	Commencement	Application, saving and transitional provisions
Telecommunications (Interception and Access) Amendment Act 2010	2, 2010	12 Feb 2010	13 Feb 2010	Sch. 2 (items 14–17)
Crimes Legislation Amendment (Serious and Organised Crime) Act 2010	3, 2010	19 Feb 2010	Schedule 4 (items 14–16, 16A, 17, 18, 18A–18H, 18J): Royal Assent	Sch 4 (items 18, 18J)
Crimes Legislation Amendment (Serious and Organised Crime) Act (No. 2) 2010	4, 2010	19 Feb 2010	Schedule 4 (item 4) and Schedule 7 (items 25, 29): 20 Feb 2010	Sch 7 (item 29)
Statute Law Revision Act 2010	8, 2010	1 Mar 2010	Schedule 1 (items 48–52) and Schedule 5 (item 123): Royal Assent	—
Crimes Legislation Amendment (Sexual Offences Against Children) Act 2010	42, 2010	14 Apr 2010	Schedule 1 (items 75–78): 15 Apr 2010	Sch. 1 (item 78)
Trade Practices Amendment (Australian Consumer Law) Act (No. 1) 2010	44, 2010	14 Apr 2010	Schedule 4 (item 2): 1 July 2010	—
Anti-People Smuggling and Other Measures Act 2010	50, 2010	31 May 2010	Schedule 1 (items 17, 18) and Schedule 3: 1 June 2010	—
Freedom of Information Amendment (Reform) Act 2010	51, 2010	31 May 2010	Sch 5 (item 76) and Sch 7: 1 Nov 2010 (s 2(1) item 7)	Sch 7
Trade Practices Amendment (Australian Consumer Law) Act (No. 2) 2010	103, 2010	13 July 2010	Schedule 6 (items 1, 140): 1 Jan 2011	—

Endnote 3—Legislation history

Act	Number and year	Assent	Commencement	Application, saving and transitional provisions
Corporations Amendment (No. 1) Act 2010	131, 2010	24 Nov 2010	Schedule 1 (item 21): 13 Dec 2010 (<i>see</i> F2010L03188)	—
Crimes Legislation Amendment Act 2011	2, 2011	2 Mar 2011	Schedule 1 (items 5–8): Royal Assent	Sch. 1 (items 7, 8)
Law and Justice Legislation Amendment (Identity Crimes and Other Measures) Act 2011	3, 2011	2 Mar 2011	Schedule 2 (item 28): 3 Mar 2011	—
Telecommunications Interception and Intelligence Services Legislation Amendment Act 2011	4, 2011	22 Mar 2011	Schedules 1–5, Schedule 6 (items 28, 29) and Schedule 7: 23 Mar 2011	Sch 1 (items 28, 29), Sch 2 (item 9), Sch 3 (item 9), Sch 4 (item 4), Sch 5 (item 37) and Sch 6 (item 29)
Acts Interpretation Amendment Act 2011	46, 2011	27 June 2011	Schedule 2 (item 1140) and Schedule 3 (items 10, 11): 27 Dec 2011	Sch 3 (items 10, 11)
Extradition and Mutual Assistance in Criminal Matters Legislation Amendment Act 2012	7, 2012	20 Mar 2012	Sch 3 (items 42–49): 20 Sept 2012 (s 2(1) item 6)	Sch 3 (item 49)
Telecommunications Interception and Other Legislation Amendment (State Bodies) Act 2012	74, 2012	27 June 2012	Sch 1 (items 4–25), Sch 2 and 3: 10 Feb 2013 (s 2(1) items 2, 9, 10) Sch 4: 20 Dec 2012 (s 2(1) item 11)	Sch 3 (item 13)

Endnotes

Endnote 3—Legislation history

Act	Number and year	Assent	Commencement	Application, saving and transitional provisions
Cybercrime Legislation Amendment Act 2012	120, 2012	12 Sept 2012	Sch 1 (items 2–5, 8–34), Sch 2 (items 5–24, 32–53), Sch 4 and Sch 5: 10 Oct 2012 (s 2(1) items 2, 4)	Sch 1 (item 34), Sch 2 (items 24, 51–53), Sch 4 (item 4) and Sch 5 (item 4)
Law Enforcement Integrity Legislation Amendment Act 2012	194, 2012	12 Dec 2012	Sch 1 (items 79–90, 91(3)–(6)): 13 Dec 2012 (s 2(1) item 4)	Sch 1 (item 91(3)–(6))
Crimes Legislation Amendment (Slavery, Slavery-like Conditions and People Trafficking) Act 2013	6, 2013	7 Mar 2013	Sch 2 (item 15) and Sch 3: 8 Mar 2013 (s 2)	Sch 3
Federal Circuit Court of Australia (Consequential Amendments) Act 2013	13, 2013	14 Mar 2013	Sch 1 (items 512–514): 12 Apr 2013 (s 2(1) item 2)	Sch 1 (item 514)
Crimes Legislation Amendment (Law Enforcement Integrity, Vulnerable Witness Protection and Other Measures) Act 2013	74, 2013	28 June 2013	Sch 6 (items 5–8): 29 June 2013 (s 2(1) item 7)	—
Statute Law Revision Act 2013	103, 2013	29 June 2013	Sch 1 (items 65–68): 29 June 2013 (s 2(1) item 2)	—
National Security Legislation Amendment Act (No. 1) 2014	108, 2014	2 Oct 2014	Sch 1 (items 57–87) and Sch 2 (items 48–50): 30 Oct 2014 (s 2(1) item 2)	Sch 1 (items 78–87) and Sch 2 (item 50)
Counter-Terrorism Legislation Amendment (Foreign Fighters) Act 2014	116, 2014	3 Nov 2014	Sch 1 (items 138, 139): 1 Dec 2014 (s 2(1) item 2)	—

Endnote 3—Legislation history

Act	Number and year	Assent	Commencement	Application, saving and transitional provisions
Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015	39, 2015	13 April 2015	Sch 1 (items 1, 5–7), Sch 2 and Sch 3: 13 Oct 2015 (s 2(1) items 2, 4) Sch 1 (items 8–12): 13 Apr 2015 (s 2(1) items 1, 3)	Sch 1 (items 7–12), Sch 2 (items 48–51) and Sch 3 (items 8–10)
Customs and Other Legislation Amendment (Australian Border Force) Act 2015	41, 2015	20 May 2015	Sch 5 (items 162–170), Sch 6 (items 188, 189) and Sch 9: 1 July 2015 (s 2(1) items 2, 7) Sch 8 (items 10–13): 13 Oct 2015 (s 2(1) item 6)	Sch 6 (item 189) and Sch 9
as amended by				
Australian Border Force Amendment (Protected Information) Act 2017	115, 2017	30 Oct 2017	Sch 1 (item 26): 1 July 2015 (s 2(1) item 2)	—
Tribunals Amalgamation Act 2015	60, 2015	26 May 2015	Sch 8 (items 51, 52) and Sch 9: 1 July 2015 (s 2(1) items 19, 22)	Sch 9
Acts and Instruments (Framework Reform) (Consequential Provisions) Act 2015	126, 2015	10 Sept 2015	Sch 1 (items 626, 627): 5 Mar 2016 (s 2(1) item 2)	—
Statute Law Revision Act (No. 2) 2015	145, 2015	12 Nov 2015	Sch 3 (item 38): 10 Dec 2015 (s 2(1) item 7)	—
Crimes Legislation Amendment (Powers, Offences and Other Measures) Act 2015	153, 2015	26 Nov 2015	Sch 15 (items 34–51, 53): 27 Nov 2015 (s 2(1) items 3, 5) Sch 15 (item 52): never commenced (s 2(1) item 4)	—

Telecommunications (Interception and Access) Act 1979

683

Compilation No. 117

Compilation date: 02/04/2022

Registered: 26/04/2022

Endnotes

Endnote 3—Legislation history

Act	Number and year	Assent	Commencement	Application, saving and transitional provisions
Territories Legislation Amendment Act 2016	33, 2016	23 Mar 2016	Sch 5 (item 93): 1 July 2016 (s 2(1) item 7)	—
Counter-Terrorism Legislation Amendment Act (No. 1) 2016	82, 2016	29 Nov 2016	Sch 9: 30 Nov 2016 (s 2(1) item 2)	Sch 9 (items 59, 60)
as amended by				
Criminal Code Amendment (High Risk Terrorist Offenders) Act 2016	95, 2016	7 Dec 2016	Sch 2 (items 16, 17): never commenced (s 2(1) item 5)	—
Law Enforcement Legislation Amendment (State Bodies and Other Measures) Act 2016	86, 2016	30 Nov 2016	Sch 1 (items 1, 56–58): 1 Dec 2016 (s 2(1) items 2, 4) Sch 1 (items 2–36, 54, 55): 1 July 2017 (s 2(1) item 3)	Sch 1 (items 1, 29–36, 54–58)
Criminal Code Amendment (High Risk Terrorist Offenders) Act 2016	95, 2016	7 Dec 2016	Sch 2 (items 2–11, 18–23): 7 June 2017 (s 2(1) items 3, 6, 7) Sch 2 (items 12–15): never commenced (s 2(1) item 4)	—
Criminal Code Amendment (Protecting Minors Online) Act 2017	50, 2017	22 June 2017	Sch 2 (item 3): 23 June 2017 (s 2(1) item 1)	—
Statute Update (Winter 2017) Act 2017	93, 2017	23 Aug 2017	Sch 1 (items 19, 20): 20 Sept 2017 (s 2(1) item 2)	—

Endnote 3—Legislation history

Act	Number and year	Assent	Commencement	Application, saving and transitional provisions
Telecommunications and Other Legislation Amendment Act 2017	111, 2017	18 Sept 2017	Sch 1 (items 30, 31, 35): 18 Sept 2018 (s 2(1) item 2)	Sch 1 (item 35)
as amended by				
Home Affairs and Integrity Agencies Legislation Amendment Act 2018	31, 2018	9 May 2018	Sch 2 (item 283): 18 Sept 2018 (s 2(1) item 6) Sch 2 (item 284): 11 May 2018 (s 2(1) item 7)	Sch 2 (item 284)
Home Affairs and Integrity Agencies Legislation Amendment Act 2018	31, 2018	9 May 2018	Sch 2 (items 224–239, 284): 11 May 2018 (s 2(1) items 3, 7) Sch 2 (items 242–249): 22 Nov 2018 (s 2(1) item 4)	Sch 2 (item 284)
Crimes Legislation Amendment (International Crime Cooperation and Other Measures) Act 2018	34, 2018	22 May 2018	Sch 1 (items 7–11, 30–70, 75–79): 22 Nov 2018 (s 2(1) item 2) Sch 6 (items 20–22, 31, 32): 23 May 2018 (s 2(1) item 8)	Sch 1 (items 11, 60, 70, 79) and Sch 6 (items 31, 32)
Investigation and Prosecution Measures Act 2018	37, 2018	22 May 2018	Sch 1 (items 1–10, 16–18): 22 May 2018 (s 2(1) item 2)	Sch 1 (items 1, 6–10, 16–18)
National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018	67, 2018	29 June 2018	Sch 4 (items 1, 2): 30 June 2018 (s 2(1) item 5) Sch 4 (item 3): 29 Dec 2018 (s 2(1) item 6)	—
Unexplained Wealth Legislation Amendment Act 2018	126, 2018	3 Oct 2018	Sch 6: 10 Dec 2018 (s 2(1) item 2)	Sch 6 (item 9)

Telecommunications (Interception and Access) Act 1979

685

Compilation No. 117

Compilation date: 02/04/2022

Registered: 26/04/2022

Endnotes

Endnote 3—Legislation history

Act	Number and year	Assent	Commencement	Application, saving and transitional provisions
Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018	148, 2018	8 Dec 2018	Sch 1 (items 7C–7G) and Sch 2 (items 120–123, 123A, 123B, 123BA, 123C, 123D, 124, 124A, 125, 126, 126AA, 126A, 127–131, 131A, 132): 9 Dec 2018 (s 2(1) items 2, 4)	Sch 2 (item 132)
Combatting Child Sexual Exploitation Legislation Amendment Act 2019	72, 2019	20 Sept 2019	Sch 2 (item 9) and Sch 7 (items 42–48): 21 Sept 2019 (s 2(1) items 3, 4)	Sch 7 (items 45–48)
Australian Crime Commission Amendment (Special Operations and Special Investigations) Act 2019	114, 2019	10 Dec 2019	Sch 1 (items 63–68): 10 Dec 2019 (s 2(1) item 1)	Sch 1 (item 68)
Telecommunications (Interception and Access) Amendment (Assistance and Access Amendments Review) Act 2019	124, 2019	12 Dec 2019	Sch 1 (items 2–4): 13 Dec 2019 (s 2(1) item 1)	Sch 1 (item 4)
Financial Sector Reform (Hayne Royal Commission Response—Stronger Regulators (2019 Measures)) Act 2020	3, 2020	17 Feb 2020	Sch 2: 18 Feb 2020 (s 2(1) item 1)	Sch 2 (item 12)
Radiocommunications Legislation Amendment (Reform and Modernisation) Act 2020	151, 2020	17 Dec 2020	Sch 6 (items 37, 38, 41–49): 17 June 2021 (s 2(1) items 8, 10) Sch 6 (item 50): 18 Dec 2020 (s 2(1) item 11)	Sch 6 (items 41–50)

Endnote 3—Legislation history

Act	Number and year	Assent	Commencement	Application, saving and transitional provisions
Online Safety (Transitional Provisions and Consequential Amendments) Act 2021	77, 2021	23 July 2021	Sch 2 (item 98): 23 Jan 2022 (s 2(1) item 3)	—
Telecommunications Legislation Amendment (International Production Orders) Act 2021	78, 2021	23 July 2021	Sch 1 (items 14, 15, 19–44, 47–49): 24 July 2021 (s 2(1) items 2, 4) Sch 1 (item 45): 1 Sept 2021 (s 2(1) item 3)	Sch 1 (items 44, 49)
Foreign Intelligence Legislation Amendment Act 2021	95, 2021	2 Sept 2021	Sch 1, Sch 2 (items 3–9) and Sch 3: 21 Dec 2021 (s 2(1) item 1)	Sch 1 (item 14), Sch 2 (item 9) and Sch 3 (item 7)
Surveillance Legislation Amendment (Identify and Disrupt) Act 2021	98, 2021	3 Sept 2021	Sch 1 (items 52–62), Sch 2 (items 112–122) and Sch 5 (items 7, 8): 4 Sept 2021 (s 2(1) items 2–4)	—
Counter-Terrorism Legislation Amendment (High Risk Terrorist Offenders) Act 2021	131, 2021	8 Dec 2021	Sch 1 (items 313–392, 394–397) and Sch 2: 9 Dec 2021 (s 2(1) items 2, 3)	—
National Security Legislation Amendment (Comprehensive Review and Other Measures No. 1) Act 2022	31, 2022	1 Apr 2022	Sch 13 (items 3–6): 2 Apr 2022 (s 2(1) item 8)	Sch 13 (item 6)

Endnotes

Endnote 4—Amendment history

Endnote 4—Amendment history

Provision affected	How affected
Title	am No 63, 1985; No 102, 1986 (as am by No 28, 1991); No 40, 2006; No 78, 2021
Chapter 1	
Part I heading	rep No 40, 2006
Chapter 1 heading.....	ad No 40, 2006
Part 1-1	
Part 1-1 heading.....	ad No 40, 2006
s 1	am No 40, 2006
s 2	am No 161, 1999
s 3	rep No 89, 1987
s 4	rs No 145, 2015
s 4A	ad No 24, 2001
s 4B	ad No 33, 2016 <u>(1) exp (s 4B(2))</u>
Part 1-2	
Part IA heading.....	ad No 89, 1987 rep No 40, 2006
Part 1-2 heading.....	ad No 40, 2006
s 5	am No 181, 1979; No 102, 1986; No 89, 1987; No 120, 1987; No 121, 1988; No 63, 1989; No 11, 1990; No 28, 1991; No 99, 1991; No 103, 1993; No 170, 1994; No 141, 1995; No 59, 1997; No 160, 1997; No 89, 1999; No 146, 1999; No 151, 1999; No 161, 1999; No 9, 2000; No 63, 2000; No 55, 2001; No 135, 2001; No 166, 2001; No 67, 2002; No 125, 2002; No 113, 2003; No 55, 2004; No 127, 2004; No 95, 2005; No 100, 2005; No 129, 2005; No 152, 2005; No 40, 2006; No 86, 2006; No 177, 2007; No 95, 2008; No 32, 2009; No 2, 2010; No 3, 2010; No 8, 2010; No 50, 2010; No 2, 2011; No 4, 2011; No 74, 2012; No 120, 2012; No 194, 2012; No 74, 2013; No 103, 2013; No 108, 2014; No 39, 2015; No 41, 2015; No 153, 2015; No 82, 2016; No 86, 2016; No 95, 2016; No 31, 2018; No 34, 2018; No 37, 2018; No 126, 2018; No 148, 2018

Endnote 4—Amendment history

Provision affected	How affected
	ed C106
	am No 114, 2019; No 3, 2020; No 78, 2021; No 95, 2021; No 98, 2021; No 131, 2021
s 5AA	ad No 166, 2001
s 5AB.....	ad No 177, 2007
	am No 120, 2012
s 5AC.....	ad No 95, 2008
	am No 32, 2009; No 74, 2012; No 86, 2016; No 37, 2018
s 5AD	ad No 95, 2008
	am No 108, 2014
s 5AE.....	ad No 95, 2008
s 5A	ad No 89, 1987
	am No 103, 1993; No 78, 2021
s 5B	ad No 89, 1987
	am No 5, 1988; No 11, 1990; No 170, 1994; No 19, 1995; No 160, 1997; No 63, 2000; No 166, 2001; No 42, 2002; No 67, 2002; No 113, 2003; No 100, 2005; No 152, 2005; No 40, 2006; No 177, 2007; No 2, 2010; No 3, 2010; No 4, 2010; No 74, 2012; No 194, 2012; No 153, 2015; No 82, 2016; No 86, 2016, No 95, 2016; No 126, 2018; No 131, 2021
s 5C	ad No 89, 1987
	am No 40, 2006; No 39, 2015
s 5D	ad No 141, 1995
	am No 89, 1999; No 137, 2000; No 161, 2001; No 67, 2002; No 86, 2002; No 113, 2003; No 55, 2004; No 127, 2004; No 96, 2005; No 129, 2005; No 152, 2005; No 40, 2006; No 86, 2006; No 3, 2007; No 177, 2007; No 59, 2009; No 3, 2010; No 4, 2010; No 42, 2010; No 44, 2010; No 50, 2010; No 103, 2010; No 131, 2010; No 3, 2011; No 6, 2013; No 116, 2014; No 50, 2017; No 93, 2017; No 34, 2018; No 67, 2018; No 72, 2019; No 114, 2019; No 3, 2020; No 131, 2021
s 5E.....	ad No 40, 2006
s 5EA.....	ad No 120, 2012
	rep No 34, 2018

Endnotes

Endnote 4—Amendment history

Provision affected	How affected
s 5F.....	ad No 40, 2006 am No 177, 2007; No 23, 2008; No 2, 2010; No 78, 2021
s 5G.....	ad No 40, 2006 am No 177, 2007; No 23, 2008; No 2, 2010; No 78, 2021
s 5H.....	ad No 40, 2006
s 6.....	am No 89, 1987; No 121, 1988; No 63, 1989; No 103, 1993; No 67, 2002; No 55, 2004; No 95, 2005; No 40, 2006; No 126, 2015; No 151, 2020; No 78, 2021
s 6AAA.....	ad No 2, 2010
s 6AA.....	ad No 40, 2006
s 6A.....	ad No 89, 1987 am No 11, 1990; No 28, 1991; No 103, 1993; No 170, 1994; No 160, 1997; No 151, 1999; No 63, 2000; Nos 67 and 125, 2002; No 113, 2003; Nos 100 and 152, 2005; No 86, 2006; No 74, 2012; No 153, 2015; No 86, 2016
s 6B.....	ad No 89, 1987
s 6C.....	ad No 89, 1987
s 6D.....	ad No 89, 1987 am No 120, 1987; No 65, 1988; No 31, 2018; No 78, 2021
s 6DA.....	ad No 160, 1997 am No 55, 2004; No 40, 2006; No 60, 2015; No 31, 2018; No 78, 2021
s 6DB.....	ad No 40, 2006 am No 13, 2013; No 60, 2015; No 31, 2018; No 78, 2021
s 6DC.....	ad No 39, 2015 am No 31, 2018
s 6E.....	ad No 89, 1987 am No 120, 1987; No 66, 1988; No 103, 1993; No 148, 2004; No 152, 2005; No 40, 2006; No 2, 2010; No 78, 2021
s 6EA.....	ad No 141, 1995 am No 40, 2006
s 6EAA.....	ad No 120, 2012

Endnote 4—Amendment history

Provision affected	How affected
s 6EB.....	ad No 40, 2006
s 6F.....	ad No 89, 1987
s 6G.....	ad No 89, 1987 am No 152, 2005
s 6H.....	ad No 89, 1987 am No 160, 1997; No 63, 2000; No 67, 2002; No 40, 2006; No 120, 2012; No 82, 2016; No 131, 2021
s 6J.....	ad No 89, 1987
s 6K.....	ad No 89, 1987 am No 160, 1997; Nos 67 and 86, 2002; Nos 95 and 129, 2005
s 6L.....	ad No 89, 1987 am No 11, 1990; No 28, 1991; No 103, 1993; No 170, 1994; No 160, 1997; No 151, 1999; No 63, 2000; Nos 67, 86 and 125, 2002; No 113, 2003; Nos 100 and 152, 2005; Nos 40 and 86, 2006; No 3, 2010; No 74, 2012; No 153, 2015; No 86, 2016; No 126, 2018
s 6M.....	ad No 89, 1987
s 6N.....	ad No 103, 1993 am No 9, 2000
s 6P.....	ad No 63, 2000 am No 78, 2021
s 6Q.....	ad No 40, 2006
s 6R.....	ad No 177, 2007 am No 39, 2015
s 6S.....	ad No 194, 2012 am No 41, 2015
s 6T.....	ad No 82, 2016 rs No 131, 2021
s 6U.....	ad No 82, 2016 rs No 131, 2021
Chapter 2	
Part II heading.....	am No 103, 1993 rep No 40, 2006

Endnotes

Endnote 4—Amendment history

Provision affected	How affected
Chapter 2 heading.....	ad No 40, 2006
Part 2-1	
Part 2-1 heading.....	ad No 40, 2006
s 7.....	am No 181, 1979; No 114, 1983; No 63, 1985; No 102, 1986; No 89, 1987; No 121, 1988; No 63, 1989; No 28, 1991; No 103, 1993; No 141, 1995; No 43, 1996; No 160, 1997; No 161, 1999; Nos 127 and 148, 2004; No 152, 2005; No 40, 2006; No 177, 2007; No 2, 2010; No 108, 2014; No 82, 2016; No 148, 2018; No 78, 2021; No 98, 2021; No 131, 2021
s 7A.....	ad No 116, 1983 am No 6, 1984 rep No 89, 1987
s 7B.....	ad No 116, 1984 am No 8, 1985 rep No 89, 1987
s 7BA.....	ad No 8, 1985 am No 63, 1985 rep No 89, 1987
s 7C.....	ad No 116, 1984 rep No 89, 1987
s 8.....	am No 181, 1979; No 89, 1987; No 65, 1988; No 121, 1988; No 99, 1991 rep No 103, 1993
Part IIA.....	ad No 120, 1987 rep No 103, 1993
s 8A, 8B.....	ad No 120, 1987 rep No 103, 1993
s 8C.....	ad No 120, 1987 am No 120, 1987 rep No 103, 1993
s 8D–8H.....	ad No 120, 1987 rep No 103, 1993

Endnote 4—Amendment history

Provision affected	How affected
s 8J	ad No 120, 1987 am No 120, 1987 rep No 103, 1993
Part 2-2	
Part III heading	am No 103, 1993 rs No 161, 1999 rep No 40, 2006
Part 2-2 heading	ad No 40, 2006
s 9	am No 121, 1988; No 63, 1989; No 43, 1996; No 161, 1999; No 63, 2000; No 40, 2006; No 31, 2018
s 9A	ad No 63, 2000 am No 40, 2006; No 177, 2007; No 23, 2008; No 31, 2018
s 9B	ad No 63, 2000 am No 40, 2006; No 31, 2018
s 10	am No 43, 1996; No 161, 1999; No 63, 2000; No 128, 2005; No 40, 2006; No 31, 2018
s 11	am No 89, 1987; No 121, 1988; No 63, 1989; No 99, 1991 rep No 103, 1993
s 11A	ad No 102, 1986 am No 89, 1987; No 121, 1988; No 63, 1989; No 99, 1991; No 103, 1993; No 161, 1999; No 63, 2000; No 50, 2010; No 31, 2018; No 95, 2021
s 11B	ad No 63, 2000 am No 40, 2006; No 23, 2008; No 50, 2010; No 31, 2018; No 95, 2021
s 11C	ad No 63, 2000 am No 50, 2010; No 31, 2018; No 95, 2021
s 11D	ad No 63, 2000 am No 127, 2004; No 31, 2018; No 95, 2021
s 12	am No 102, 1986; No 43, 1996; No 161, 1999; No 63, 2000; No 40, 2006; No 108, 2014; No 31, 2022

Endnotes

Endnote 4—Amendment history

Provision affected	How affected
s 13	am No 102, 1986; No 89, 1987; No 103, 1993; No 43, 1996; No 63, 2000; No 40, 2006; No 31, 2018
s 14	rs No 102, 1986 am No 89, 1987; No 103, 1993; No 161, 1999; No 63, 2000; No 40, 2006; No 95, 2021
s 15	am No 102, 1986; No 89, 1987; No 121, 1988; No 63, 1989 (as am by No 11, 1991); No 99, 1991; No 103, 1993; No 43, 1996; No 161, 1999; No 63, 2000; No 55, 2004; No 40, 2006; No 4, 2011; No 31, 2018; No 95, 2021
s 16	am No 102, 1986 rep No 89, 1987 ad No 63, 2000 am No 40, 2006; No 23, 2008; No 4, 2011
s 17	am No 102, 1986; No 89, 1987; No 28, 1991; No 103, 1993; No 161, 1999; No 63, 2000; No 40, 2006; No 31, 2018
s 18	ad No 103, 1993 am No 161, 1999; No 55, 2001; No 2, 2010; No 108, 2014 ed C93
Part IV heading.....	am No 181, 1979; No 89, 1987 rep No 103, 1993
Part IV	rep No 103, 1993
s 18, 19	rep No 89, 1987
s 20	am No 181, 1979 rep No 89, 1987
s 20A, 20B.....	ad No 89, 1987 am No 121, 1988; No 99, 1991 rep No 103, 1993
s 21	am No 181, 1979; No 89, 1987; No 121, 1988; No 63, 1989; No 99, 1991 rep No 103, 1993
s 22	am No 181, 1979 rep No 89, 1987

Endnote 4—Amendment history

Provision affected	How affected
s 23	am No 181, 1979 rs No 89, 1987 rep No 103, 1993
s 24	am No 181, 1979 rep No 89, 1987
s 25	am No 181, 1979; No 89, 1987; No 63, 1989; No 99, 1991 rep No 103, 1993
s 25A	ad No 63, 1985 rep No 89, 1987
s 26	rep No 89, 1987
s 27	am No 181, 1979 rep No 89, 1987
s 28	rep No 89, 1987
Part 2-3	
Part V heading	am No 121, 1988 rs No 67, 2002 rep No 40, 2006
Part 2-3 heading	ad No 40, 2006
Part V	ad No 63, 1985
s 29	ad No 63, 1985 rep No 89, 1987
s 30	ad No 63, 1985 am No 89, 1987; No 121, 1988; No 63, 1989
Part 2-4	
Part 2-4	ad No 177, 2007
s 31	ad No 63, 1985 rep No 89, 1987 ad No 177, 2007 am No 31, 2018; No 148, 2018
s 31A	ad No 177, 2007 am No 31, 2018; No 148, 2018

Endnotes

Endnote 4—Amendment history

Provision affected	How affected
s 31AA	ad No 148, 2018
s 31B	ad No 177, 2007
s 31C	ad No 177, 2007
s 31D	ad No 177, 2007 am No 31, 2018
s 31E.....	ad No 148, 2018
Part 2-5	
Part VI heading.....	rs No 67, 2002 rep No 40, 2006
Part 2-5 heading.....	ad No 40, 2006
Part VI.....	ad No 89, 1987
Division 1	rep No 40, 2006
s 32	ad No 89, 1987 rep No 40, 2006
s 33	ad No 89, 1987 rs No 103, 1993 am No 67, 2002 rep No 40, 2006
Division 2	
s 34	ad No 89, 1987 am No 3, 1995; No 152, 2005; No 82, 2016; No 131, 2021
s 35	ad No 89, 1987 am No 121, 1988; No 63, 1989; No 11, 1990; No 28, 1991; No 63, 2000; No 135, 2001; No 125, 2002; No 40, 2006; No 23, 2008; No 32, 2009; Nos 2 and 8, 2010; No 74, 2012; No 82, 2016
s 36	ad No 89, 1987 am No 99, 1988 rep No 152, 2005 ad No 23, 2008
s 37	ad No 89, 1987
s 38	ad No 89, 1987

Endnote 4—Amendment history

Provision affected	How affected
s 38A	ad No 82, 2016 am No 131, 2021 ed C114
Division 3	
s 39	ad No 89, 1987 am No 11, 1990; No 28, 1991; No 103, 1993; No 160, 1997; No 151, 1999; No 63, 2000; Nos 67 and 125, 2002; No 113, 2003; Nos 100 and 152, 2005; No 86, 2006; No 95, 2008; No 74, 2012; No 103, 2013; No 153, 2015; No 86, 2016
s 40, 41	ad No 89, 1987
s 42	ad No 89, 1987 am No 63, 2000; No 40, 2006; No 23, 2008
s 43	ad No 89, 1987 am No 160, 1997
s 44	ad No 89, 1987 (as am by No 11, 1991) am No 160, 1997
s 44A	ad No 74, 2012 am No 82, 2016; No 131, 2021
s 45	ad No 89, 1987 am No 160, 1997; No 63, 2000 rep No 40, 2006 ad No 32, 2009 am No 74, 2012; No 82, 2016; No 131, 2021
s 45A	ad No 63, 2000 rep No 40, 2006 ad No 32, 2009 rs No 74, 2012
Division 4	
s 46	ad No 89, 1987 am No 160, 1997; No 63, 2000; No 40, 2006; No 32, 2009; No 74, 2012; No 82, 2016; No 131, 2021
s 46A	ad No 63, 2000

Telecommunications (Interception and Access) Act 1979

697

Compilation No. 117

Compilation date: 02/04/2022

Registered: 26/04/2022

Endnotes

Endnote 4—Amendment history

Provision affected	How affected
	am No 40, 2006; No 23, 2008; No 32, 2009; No 74, 2012; No 82, 2016; No 131, 2021
s 47	ad No 89, 1987
	am No 121, 1988
	rs No 63, 1989
	am No 103, 1993; Nos 9 and 63, 2000; No 67, 2002; No 40, 2006
	rs No 40, 2006
	am No 4, 2011
s 48	ad No 89, 1987
	am No 121, 1988; No 63, 1989; No 28, 1991; No 160, 1997; No 63, 2000; No 67, 2002; No 40, 2006; No 82, 2016; No 131, 2021
s 49	ad No 89, 1987
	am No 160, 1997; No 63, 2000; No 67, 2002; No 40, 2006; No 82, 2016; No 131, 2021
s 50	ad No 89, 1987
	am No 11, 1990; No 160, 1997
s 51	ad No 89, 1987
	am No 160, 1997
s 52	ad No 89, 1987
	am No 103, 1993; No 160, 1997; No 63, 2000; No 40, 2006; No 23, 2008; No 4, 2011
s 53	ad No 89, 1987
	am No 103, 1993; No 160, 1997; No 63, 2000; No 40, 2006
	rep No 23, 2008
s 54	ad No 89, 1987
	rs No 103, 1993
	am No 63, 2000; No 67, 2002; No 40, 2006
	rs No 40, 2006
s 55	ad No 89, 1987
	am No 11, 1990
	rs No 103, 1993

Endnote 4—Amendment history

Provision affected	How affected
	am No 160, 1997; No 63, 2000; No 55, 2004; No 40, 2006; No 4, 2011; No 108, 2014
s 56	ad No 89, 1987
	am No 103, 1993; No 63, 2000
	rep No 40, 2006
s 57	ad No 89, 1987
	am No 103, 1993; No 63, 2000; No 40, 2006; No 23, 2008; No 4, 2011; No 82, 2016; No 131, 2021
s 58	ad No 89, 1987
	am No 63, 2000; No 67, 2002; No 40, 2006; No 4, 2011
s 59	ad No 89, 1987
	am No 40, 2006; No 4, 2011
s 59A	ad No 23, 2008
s 59B	ad No 82, 2016
	rs No 131, 2021
s 60	ad No 89, 1987
	rs No 63, 1989
	am No 28, 1991; No 103, 1993; No 63, 2000; No 67, 2002; No 55, 2004; No 40, 2006; No 23, 2008; No 4, 2011
s 61	ad No 89, 1987
	am No 121, 1988; No 63, 1989; No 103, 1993; No 63, 2000; No 55, 2001; No 67, 2002; No 40, 2006; No 177, 2007; No 4, 2011
s 61A	ad No 66, 1988
	am No 103, 1993
Part 2-6	
Part VII heading	rep No 40, 2006
Part 2-6 heading.....	ad No 40, 2006
Part VII.....	ad No 89, 1987
s 62	ad No 89, 1987
s 63	ad No 89, 1987
	am No 121, 1988; No 63, 1989 (as am by No 11, 1991); No 141, 1995; No 40, 2006; No 82, 2016

Endnotes

Endnote 4—Amendment history

Provision affected	How affected
s 63AA	ad No 141, 1995 am No 40, 2006
s 63AB.....	ad No 148, 2018 am No 95, 2021; No 98, 2021
s 63AC.....	ad No 148, 2018 am No 95, 2021; No 98, 2021
s 63AD	ad No 98, 2021
s 63AE.....	ad No 98, 2021
s 63A	ad No 120, 1987 am No 103, 1993
s 63B	ad No 63, 1989 am No 141, 1995; No 40, 2006; No 148, 2018
s 63C–63E	ad No 2, 2010
s 64	ad No 89, 1987 am No 141, 1995; No 161, 1999; No 63, 2000; No 40, 2006; No 4, 2011; No 108, 2014; No 39, 2015; No 148, 2018
s 65	ad No 89, 1987 am No 141, 1995; No 161, 1999; No 63, 2000; No 77, 2003; No 40, 2006; No 4, 2011; No 31, 2018; No 148, 2018; No 95, 2021
s 65A	ad No 120, 1987 am Nos 66 and 121, 1988; No 63, 1989 rs No 103, 1993 am No 141, 1995; No 63, 2000; No 40, 2006 rs No 82, 2016 am No 148, 2018; No 131, 2021
s 66	ad No 89, 1987 am No 4, 2011
s 67	ad No 89, 1987 am No 141, 1995; No 160, 1997; No 63, 2000; No 166, 2001; No 40, 2006; No 4, 2011; No 82, 2016; No 148, 2018; No 3, 2020; No 98, 2021; No 131, 2021
s 68	ad No 89, 1987

Endnote 4—Amendment history

Provision affected	How affected
	am No 170, 1994; No 141, 1995; No 160, 1997; No 151, 1999; No 63, 2000; No 166, 2001; No 67, 2002; No 113, 2003; Nos 100 and 152, 2005; Nos 40 and 86, 2006; No 3, 2010; No 2, 2011; Nos 7, 74 and 194, 2012; No 41, 2015; No 153, 2015; No 86, 2016; No 31, 2018; No 34, 2018; No 37, 2018; No 126, 2018; No 148, 2018; No 3, 2020; No 98, 2021
s 68A	ad No 7, 2012
	am No 31, 2018
	rs No 34, 2018
s 69	ad No 89, 1987
s 70	ad No 89, 1987
	am No 40, 2006
s 71	ad No 89, 1987
	am No 135, 2001; No 125, 2002; No 86, 2006; No 31, 2018
s 72	ad No 89, 1987
	am No 120, 1987; No 63, 1989; No 2, 2010
s 73	ad No 89, 1987
	am No 120, 1987; No 63, 1989; No 28, 1991; No 2, 2010
s 74	ad No 89, 1987
	am No 141, 1995; No 63, 2000; No 40, 2006; No 148, 2018; No 98, 2021
s 75	ad No 89, 1987
	am No 63, 2000; No 148, 2018; No 98, 2021
s 75A	ad No 63, 2000
s 76	ad No 89, 1987
	am No 141, 1995; No 40, 2006
s 76A	ad No 141, 1995
	am No 40, 2006
s 77	ad No 89, 1987
	am No 120, 1987; No 103, 1993; No 141, 1995; No 63, 2000; No 40, 2006; No 148, 2018; No 98, 2021
s 78	ad No 89, 1987

Telecommunications (Interception and Access) Act 1979

701

Compilation No. 117

Compilation date: 02/04/2022

Registered: 26/04/2022

Endnotes

Endnote 4—Amendment history

Provision affected	How affected
	am No 40, 2006
s 79	ad No 89, 1987
	am No 103, 1993; No 141, 1995; No 40, 2006; No 2, 2010; No 82, 2016
s 79AA	ad No 82, 2016
	am No 131, 2021
s 79A	ad No 2, 2010
Part 2-7	
Part VIII heading	rep No 40, 2006
Part 2-7 heading	ad No 40, 2006
	rs No 40, 2006
Part VIII	ad No 89, 1987
s 80	ad No 89, 1987
	am No 65, 1988; No 103, 1993; No 63, 2000; No 135, 2001; No 125, 2002; No 40, 2006
	rs No 40, 2006
	am No 23, 2008; No 8, 2010; No 82, 2016
s 81	ad No 89, 1987
	am No 65, 1988; No 28, 1991; No 103, 1993; No 160, 1997; No 63, 2000; No 135, 2001; No 125, 2002; No 40, 2006
	rs No 40, 2006
	am No 2, 2010; No 4, 2011; No 82, 2016
	ed C92
s 81AA	ad No 4, 2011
s 81A	ad No 103, 1993
	am No 141, 1995; No 160, 1997; No 63, 2000; No 67, 2002; No 40, 2006; No 82, 2016; No 131, 2021
s 81B	ad No 103, 1993
	am No 141, 1995; No 40, 2006
s 81C	ad No 141, 1995
	am No 160, 1997; No 63, 2000; No 67, 2002; No 40, 2006; No 82, 2016; No 131, 2021

Endnote 4—Amendment history

Provision affected	How affected
s 81D	ad No 141, 1995 am No 40, 2006
s 81E.....	ad No 141, 1995 am No 40, 2006
s 82	ad No 89, 1987 am No 103, 1993; No 141, 1995 rep No 40, 2006
s 83	ad No 89, 1987 am No 82, 2016; No 148, 2018; No 131, 2021
s 84	ad No 89, 1987 am No 95, 2005; No 40, 2006; No 82, 2016; No 148, 2018
s 85	ad No 89, 1987 rs No 82, 2016
s 85A	ad No 82, 2016 am No 131, 2021
s 86	ad No 89, 1987 am No 40, 2006
s 87	ad No 89, 1987 am No 39, 2015
s 88	ad No 89, 1987
s 89	ad No 89, 1987
s 90	ad No 89, 1987
s 91	ad No 89, 1987
s 92	ad No 89, 1987 am No 40, 2006
s 92A	ad No 103, 1993
Part 2-8	
Part IX heading.....	am No 103, 1993 rep No 40, 2006
Part 2-8 heading.....	ad No 40, 2006
Part IX	ad No 89, 1987

Endnotes

Endnote 4—Amendment history

Provision affected	How affected
Division 1	
s 93	ad No 89, 1987 am No 63, 1989; No 40, 2006
s 94	ad No 89, 1987 am No 28, 1991; No 103, 1993; No 141, 1995; No 63, 2000; No 40, 2006; No 23, 2008; No 7, 2012
s 94A	ad No 160, 1997 am No 40, 2006
s 94B	ad No 63, 2000
s 95	ad No 89, 1987 am No 166, 2001
s 96	ad No 89, 1987 am No 103, 1993
s 97	ad No 89, 1987 am No 121, 1988; No 63, 1989; No 103, 1993; No 63, 2000; No 40, 2006; No 95, 2008
s 98	rep No 103, 1993
Division 2	
s 99	ad No 89, 1987 am No 40, 2006
s 100	ad No 89, 1987 am No 103, 1993; No 95, 2005; No 40, 2006; No 23, 2008
s 101	ad No 89, 1987 am No 103, 1993; No 40, 2006
s 102	ad No 89, 1987 am No 141, 1995; No 166, 2001; No 40, 2006
s 102A	ad No 103, 1993
s 102B	ad No 7, 2012 rs No 34, 2018
s 103	ad No 89, 1987 rs No 103, 1993

Endnote 4—Amendment history

Provision affected	How affected
	am No 141, 1995; No 160, 1997; No 63, 2000; No 95, 2005; No 40, 2006; No 4, 2011; No 82, 2016
s 103A	ad No 160, 1997
s 103B	ad No 82, 2016
	am No 131, 2021
Division 3	
s 104	ad No 89, 1987
	am No 103, 1993; No 40, 2006
Part 2-9	
Part X heading	rep No 40, 2006
Part 2-9 heading	ad No 40, 2006
Part X	ad No 89, 1987
s 105	ad No 89, 1987
	am No 103, 1993; No 120, 2012; No 31, 2018
s 106	ad No 89, 1987
	am No 103, 1993; No 24, 2001
s 107	ad No 89, 1987
	am No 103, 1993; No 24, 2001; No 40, 2006
Part 2-10	
Part XA heading	rep No 40, 2006
Part 2-10 heading	ad No 40, 2006
Part XA	ad No 141, 1995
s 107A–107F	ad No 141, 1995
Chapter 3	
Chapter 3 heading	rs No 120, 2012
Chapter 3	ad No 40, 2006
Part 3-1A	
Part 3-1A	ad No 120, 2012
Division 1	
s 107G	ad No 120, 2012
	am No 39, 2015; No 34, 2018

Endnotes

Endnote 4—Amendment history

Provision affected	How affected
Division 2	
s 107H.....	ad No 120, 2012
s 107J.....	ad No 120, 2012 am No 39, 2015
s 107K.....	ad No 120, 2012
s 107L.....	ad No 120, 2012 am No 39, 2015
s 107M.....	ad No 120, 2012 am No 39, 2015
Division 3	
s 107N.....	ad No 120, 2012
s 107P.....	ad No 120, 2012 am No 31, 2018 rs No 34, 2018
s 107Q.....	ad No 120, 2012 am No 31, 2018; No 34, 2018
s 107R.....	ad No 120, 2012 am No 31, 2018; No 34, 2018
s 107S.....	ad No 120, 2012
Division 4	
s 107T.....	ad No 120, 2012
s 107U.....	ad No 120, 2012
s 107V.....	ad No 120, 2012
s 107W.....	ad No 120, 2012
Part 3-1	
s 108.....	ad No 40, 2006 am No 120, 2012; No 108, 2014; No 148, 2018; No 78, 2021; No 98, 2021 ed C113
Part 3-2	
s 109.....	ad No 40, 2006

Endnote 4—Amendment history

Provision affected	How affected
Part 3-3	
Part 3-3 heading.....	rs No 39, 2015
Division 1	
s 110.....	ad No 40, 2006 am No 39, 2015
s 110A.....	ad No 39, 2015 am No 41, 2015; No 153, 2015; No 86, 2016
s 110B.....	ad No 41, 2015
s 111.....	ad No 40, 2006 am No 39, 2015
s 112.....	ad No 40, 2006
s 113.....	ad No 40, 2006
s 114.....	ad No 40, 2006
s 115.....	ad No 40, 2006
Division 2	
s 116.....	ad No 40, 2006 am No 4, 2011; No 120, 2012; No 39, 2015; No 34, 2018
s 117.....	ad No 40, 2006
s 118.....	ad No 40, 2006 am No 120, 2012
s 119.....	ad No 40, 2006
Division 3	
s 120.....	ad No 40, 2006 am No 39, 2015
s 121.....	ad No 40, 2006 am No 4, 2011
s 122.....	ad No 40, 2006 am No 39, 2015
s 123.....	ad No 40, 2006 am No 95, 2008; No 4, 2011; No 39, 2015
s 124.....	ad No 40, 2006

Endnotes

Endnote 4—Amendment history

Provision affected	How affected
	am No 4, 2011
Division 4	
s 125	ad No 40, 2006
s 126	ad No 40, 2006
	am No 4, 2011
s 127	ad No 40, 2006
	am No 4, 2011; No 39, 2015
s 128	ad No 40, 2006
	am No 39, 2015
s 129	ad No 40, 2006
	am No 2, 2010
s 130	ad No 40, 2006
	am No 39, 2015
	ed C93
s 131	ad No 40, 2006
	am No 39, 2015
s 132	ad No 40, 2006
Part 3-4	
Division 1	
Division 1 heading.....	rs No 120, 2012
s 133	ad No 40, 2006
	am No 120, 2012; No 82, 2016
Division 2	
s 134	ad No 40, 2006
	rs No 120, 2012
	am No 39, 2015
s 135	ad No 40, 2006
	am No 120, 2012; No 39, 2015
s 136	ad No 40, 2006
	am No 120, 2012; No 108, 2014
s 137	ad No 40, 2006

Endnote 4—Amendment history

Provision affected	How affected
	am No 4, 2011; No 120, 2012; No 31, 2018; No 95, 2021
s 138	ad No 40, 2006
	am No 120, 2012; No 39, 2015
s 139	ad No 40, 2006
	am No 177, 2007; No 7, 2012; No 120, 2012; No 194, 2012; No 39, 2015; No 82, 2016; No 95, 2016; No 34, 2018; No 131, 2021
s 139A	ad No 194, 2012
	am No 82, 2016; No 95, 2016; No 131, 2021
s 139B	ad No 82, 2016
	am No 95, 2016
	rs No 131, 2021
s 139C	ad No 95, 2016
	am No 95, 2016
	rep No 131, 2021
s 140	ad No 40, 2006
	am No 86, 2006; No 31, 2018
s 141	ad No 40, 2006
s 142	ad No 40, 2006
	am No 194, 2012; No 82, 2016; No 95, 2016; No 131, 2021
s 142A	ad No 120, 2012
	am No 31, 2018
	rs No 34, 2018
s 143	ad No 40, 2006
s 144	ad No 40, 2006
s 145	ad No 40, 2006
s 146	ad No 40, 2006
	am No 120, 2012
Division 3	
s 147–149	ad No 40, 2006
Division 4	
s 150	ad No 40, 2006

Endnotes

Endnote 4—Amendment history

Provision affected	How affected
	am No 194, 2012; No 39, 2015; No 82, 2016; No 95, 2016; No 131, 2021
Part 3-5	
Part 3-5 heading.....	rs No 120, 2012; No 39, 2015
Division 1	
Division 1 heading.....	rs No 120, 2012; No 39, 2015
Division 1.....	rs No 39, 2015
s 150A.....	ad No 120, 2012
	rep No 39, 2015
s 151.....	ad No 40, 2006
	rs No 39, 2015
	am No 34, 2018
Division 2	
Division 2 heading.....	rs No 120, 2012
	rep No 39, 2015
Division 2.....	rep No 39, 2015
s 152.....	ad No 40, 2006
	am No 120, 2012
	rep No 39, 2015
s 153.....	ad No 40, 2006
	am No 120, 2012
	rep No 39, 2015
s 154.....	ad No 40, 2006
	rep No 39, 2015
s 155.....	ad No 40, 2006
	rep No 39, 2015
s 156.....	ad No 40, 2006
	rep No 39, 2015
s 157.....	ad No 40, 2006
	rep No 39, 2015
s 158.....	ad No 40, 2006

Endnote 4—Amendment history

Provision affected	How affected
	rep No 39, 2015
Division 3	
Division 3	ad No 120, 2012
s 158A	ad No 120, 2012
Part 3-6	
Division 1	
s 159	ad No 40, 2006 am No 7, 2012; No 39, 2015
s 160	ad No 40, 2006 am No 39, 2015
Division 2	
s 161	ad No 40, 2006
s 161A	ad No 120, 2012 am No 39, 2015
s 162	ad No 40, 2006 am No 120, 2012; No 39, 2015; No 34, 2018
s 163	ad No 40, 2006 am No 39, 2015
s 163A	am No 7, 2012 rs No 34, 2018
Division 3	
s 164	ad No 40, 2006
Part 3-7	
s 165	ad No 40, 2006
s 166	ad No 40, 2006
s 167	ad No 40, 2006
s 168	ad No 40, 2006
s 169	ad No 40, 2006
s 170	ad No 40, 2006
Chapter 4	
Chapter 4	ad No 177, 2007

Endnotes

Endnote 4—Amendment history

Provision affected	How affected
Part 4-1	
Division 1	
s 171	ad No 177, 2007 am No 120, 2012
Division 2	
s 172	ad No 177, 2007 am No 120, 2012
s 173	ad No 177, 2007
Division 3	
s 174	ad No 177, 2007 am No 108, 2014
s 175	ad No 177, 2007 am No 108, 2014
s 176	ad No 177, 2007 am No 108, 2014; No 39, 2015; No 31, 2018
Division 4	
s 176A	ad No 39, 2015 am No 41, 2015
s 177	ad No 177, 2007
s 178	ad No 177, 2007
s 178A	ad No 4, 2011
s 179	ad No 177, 2007
s 180	ad No 177, 2007 am No 120, 2012; No 39, 2015
Division 4A	
Division 4A	ad No 120, 2012
Subdivision A	
s 180A	ad No 120, 2012 am No 34, 2018
s 180B	ad No 120, 2012 am No 31, 2018; No 34, 2018

Endnote 4—Amendment history

Provision affected	How affected
Subdivision B	
s 180C	ad No 120, 2012 am No 34, 2018
s 180D	ad No 120, 2012 am No 95, 2016; No 131, 2021
Subdivision C	
Subdivision C heading	rs No 34, 2018
s 180E	ad No 120, 2012 am No 31, 2018; No 34, 2018
Division 4B	
Division 4B	ad No 120, 2012
s 180F	ad No 120, 2012 am No 39, 2015
Division 4C	
Division 4C	ad No 39, 2015
Subdivision A	
s 180G	ad No 39, 2015
s 180H	ad No 39, 2015
Subdivision B	
s 180J	ad No 39, 2015 am No 31, 2018
s 180K	ad No 39, 2015 am No 31, 2018
s 180L	ad No 39, 2015 am No 31, 2018
s 180M	ad No 39, 2015 am No 31, 2018
s 180N	ad No 39, 2015 am No 31, 2018
s 180P	ad No 39, 2015 am No 31, 2018

Endnotes

Endnote 4—Amendment history

Provision affected	How affected
Subdivision C	
s 180Q	ad No 39, 2015
s 180R	ad No 39, 2015
s 180S	ad No 39, 2015
s 180T	ad No 39, 2015
s 180U	ad No 39, 2015
s 180V	ad No 39, 2015
s 180W	ad No 39, 2015
Subdivision D	
s 180X	ad No 39, 2015 am No 31, 2018
Division 5	
s 181	ad No 177, 2007 am No 120, 2012
Division 6	
Division 6 heading	rs No 120, 2012
s 181A	ad No 120, 2012 am No 39, 2015
s 181B	ad No 120, 2012 am No 39, 2015; No 95, 2016; No 131, 2021
s 182	ad No 177, 2007 am No 4, 2011; No 120, 2012; No 39, 2015; No 95, 2016; No 131, 2021
s 182A	ad No 39, 2015
s 182B	ad No 39, 2015 am No 95, 2016; No 131, 2021
Part 4-2	
s 183	ad No 177, 2007 am No 51, 2010; No 120, 2012
s 184	ad No 177, 2007 am No 120, 2012; No 108, 2014

Endnote 4—Amendment history

Provision affected	How affected
s 185	ad No 177, 2007 am No 120, 2012; No 39, 2015
s 185A	ad No 2, 2010
s 185B	ad No 2, 2010 am No 108, 2014 ed C93
s 185C	ad No 2, 2010
s 185D	ad No 39, 2015 am No 31, 2018
s 185E	ad No 39, 2015
s 186	ad No 177, 2007 am No 4, 2011; No 120, 2012; No 39, 2015
s 186A	ad No 39, 2015
Chapter 4A	
Chapter 4A	ad No 39, 2015
s 186B	ad No 39, 2015 am No 148, 2018
s 186C	ad No 39, 2015
s 186D	ad No 39, 2015
s 186E	ad No 39, 2015
s 186F	ad No 39, 2015
s 186G	ad No 39, 2015
s 186H	ad No 39, 2015
s 186J	ad No 39, 2015
Chapter 5	
Chapter 5 heading	rs No 4, 2011
Chapter 5	ad No 177, 2007
Part 5-1	
s 187	ad No 177, 2007
Part 5-1A	
Part 5-1A	ad No 39, 2015

Endnotes

Endnote 4—Amendment history

Provision affected	How affected
Division 1	
s 187A	ad No 39, 2015 am No 77, 2021
s 187AA	ad No 39, 2015
s 187B	ad No 39, 2015
s 187BA.....	ad No 39, 2015
s 187C	ad No 39, 2015
Division 2	
s 187D	ad No 39, 2015
s 187E.....	ad No 39, 2015
s 187F.....	ad No 39, 2015
s 187G.....	ad No 39, 2015
s 187H.....	ad No 39, 2015
s 187J.....	ad No 39, 2015
Division 3	
s 187K.....	ad No 39, 2015
s 187KA	ad No 39, 2015
Division 4	
s 187KB.....	ad No 39, 2015
s 187L.....	ad No 39, 2015
s 187LA.....	ad No 39, 2015
s 187M.....	ad No 39, 2015
s 187N	ad No 39, 2015
s 187P.....	ad No 39, 2015 am No 148, 2018; No 124, 2019
Part 5-2	
s 188	ad No 177, 2007
Part 5-3	
Division 1	
s 189–191	ad No 177, 2007

Endnote 4—Amendment history

Provision affected	How affected
Division 2	
s 192	ad No 177, 2007
s 193	ad No 177, 2007
Part 5-4	
s 194	ad No 177, 2007 rep No 4, 2011
s 195	ad No 177, 2007
s 196	ad No 177, 2007
s 197	ad No 177, 2007 am No 4, 2011
s 198–202	ad No 177, 2007
Part 5-4A	
Part 5-4A	ad No 4, 2011
s 202A	ad No 4, 2011 am No 111, 2017
s 202B	ad No 4, 2011 am No 111, 2017
s 202C	ad No 4, 2011
Part 5-5	
s 203	ad No 177, 2007 am No 46, 2011
s 204, 205	ad No 177, 2007
Part 5-6	
Division 1	
s 206	ad No 177, 2007
Division 2	
s 207	ad No 177, 2007
Division 3	
s 208	ad No 177, 2007
s 209	ad No 177, 2007
s 210	ad No 177, 2007

Endnotes

Endnote 4—Amendment history

Provision affected	How affected
s 211	ad No 177, 2007
Chapter 6	
Part XI heading.....	rep No 40, 2006
Chapter 5 heading.....	ad No 40, 2006
	rep No 177, 2007
Chapter 6 heading.....	ad No 177, 2007
	rs No 82, 2016
Part XI.....	ad No 89, 1987
Part 6-1	
Part 5-1 heading.....	ad No 40, 2006
	rep No 177, 2007
Part 6-1 heading.....	ad No 177, 2007
	rs No 82, 2016
s 298.....	ad No 82, 2016
s 299.....	ad No 82, 2016
s 299A.....	ad No 78, 2021
s 108.....	ad No 89, 1987
renum s 300.....	No 40, 2006
Schedule 1	
Schedule 1.....	ad No 78, 2021
Part 1	
c 1.....	ad No 78, 2021
	am No 131, 2021
c 2.....	ad No 78, 2021
	ed C111
	am No 131, 2021
c 3.....	ad No 78, 2021
c 3A.....	ad No 78, 2021
c 3B.....	ad No 78, 2021
c 3C.....	ad No 78, 2021
c 4.....	ad No 78, 2021

Endnote 4—Amendment history

Provision affected	How affected
c 5.....	ad No 78, 2021
c 6.....	ad No 78, 2021
c 7.....	ad No 78, 2021
c 8.....	ad No 78, 2021
c 9.....	ad No 78, 2021
c 10.....	ad No 78, 2021
c 10A.....	ad No 78, 2021
c 11.....	ad No 78, 2021
c 12.....	ad No 78, 2021
c 13.....	ad No 78, 2021
c 14.....	ad No 78, 2021
c 15.....	ad No 78, 2021
c 16.....	ad No 78, 2021
c 17.....	ad No 78, 2021
c 17A.....	ad No 78, 2021
c 18.....	ad No 78, 2021
c 19.....	ad No 78, 2021
c 20.....	ad No 78, 2021
Part 2	
Division 1	
c 21.....	ad No 78, 2021
Division 2	
Subdivision A	
c 22.....	ad No 78, 2021
c 23.....	ad No 78, 2021
c 24.....	ad No 78, 2021
c 25.....	ad No 78, 2021
c 26.....	ad No 78, 2021
c 27.....	ad No 78, 2021
c 28.....	ad No 78, 2021
c 29.....	ad No 78, 2021

Endnotes

Endnote 4—Amendment history

Provision affected	How affected
Subdivision B	
c 30.....	ad No 78, 2021
c 31.....	ad No 78, 2021
c 32.....	ad No 78, 2021
Division 3	
Subdivision A	
c 33.....	ad No 78, 2021
c 34.....	ad No 78, 2021
c 35.....	ad No 78, 2021
c 36.....	ad No 78, 2021
c 37.....	ad No 78, 2021
c 38.....	ad No 78, 2021
Subdivision B	
c 39.....	ad No 78, 2021
c 40.....	ad No 78, 2021
c 41.....	ad No 78, 2021
Division 4	
Subdivision A	
c 42.....	ad No 78, 2021
c 43.....	ad No 78, 2021
c 44.....	ad No 78, 2021
c 45.....	ad No 78, 2021
c 46.....	ad No 78, 2021
c 47.....	ad No 78, 2021
Subdivision B	
c 48.....	ad No 78, 2021
c 49.....	ad No 78, 2021
c 50.....	ad No 78, 2021
Part 3	
Part 3 heading.....	am No 131, 2021

Endnote 4—Amendment history

Provision affected	How affected
Division 1	
c 51	ad No 78, 2021 am No 131, 2021
Division 2	
Division 2 heading	am No 131, 2021
Subdivision A	
c 52	ad No 78, 2021 am No 131, 2021
c 53	ad No 78, 2021 am No 131, 2021
c 54	ad No 78, 2021 am No 131, 2021
c 55	ad No 78, 2021 am No 131, 2021
c 56	ad No 78, 2021 am No 131, 2021
c 57	ad No 78, 2021
c 58	ad No 78, 2021 am No 131, 2021
c 59	ad No 78, 2021 am No 131, 2021
Subdivision B	
c 60	ad No 78, 2021 am No 131, 2021
c 61	ad No 78, 2021 am No 131, 2021
c 62	ad No 78, 2021
Division 3	
Division 3 heading	am No 131, 2021
Subdivision A	
c 63	ad No 78, 2021

Endnotes

Endnote 4—Amendment history

Provision affected	How affected
	am No 131, 2021
c 64.....	ad No 78, 2021
	am No 131, 2021
c 65.....	ad No 78, 2021
	am No 131, 2021
c 66.....	ad No 78, 2021
c 67.....	ad No 78, 2021
	am No 131, 2021
c 68.....	ad No 78, 2021
Subdivision B	
c 69.....	ad No 78, 2021
	am No 131, 2021
c 70.....	ad No 78, 2021
	am No 131, 2021
c 71.....	ad No 78, 2021
Division 4	
Division 4 heading.....	am No 131, 2021
Subdivision A	
c 72.....	ad No 78, 2021
	am No 131, 2021
c 73.....	ad No 78, 2021
	am No 131, 2021
c 74.....	ad No 78, 2021
	am No 131, 2021
c 75.....	ad No 78, 2021
c 76.....	ad No 78, 2021
	am No 131, 2021
c 77.....	ad No 78, 2021
Subdivision B	
c 78.....	ad No 78, 2021
	am No 131, 2021

Endnote 4—Amendment history

Provision affected	How affected
c 79	ad No 78, 2021
	am No 131, 2021
c 80	ad No 78, 2021
Division 5	
Division 5 heading	am No 131, 2021
c 81	ad No 78, 2021
	am No 131, 2021
Part 4	
Division 1	
c 82	ad No 78, 2021
Division 2	
Subdivision A	
c 83	ad No 78, 2021
c 84	ad No 78, 2021
c 85	ad No 78, 2021
c 86	ad No 78, 2021
c 87	ad No 78, 2021
c 88	ad No 78, 2021
Subdivision B	
c 89	ad No 78, 2021
c 90	ad No 78, 2021
c 91	ad No 78, 2021
Division 3	
Subdivision A	
c 92	ad No 78, 2021
c 93	ad No 78, 2021
c 94	ad No 78, 2021
c 95	ad No 78, 2021
c 96	ad No 78, 2021
c 97	ad No 78, 2021

Endnotes

Endnote 4—Amendment history

Provision affected	How affected
Subdivision B	
c 98.....	ad No 78, 2021
c 99.....	ad No 78, 2021
c 100.....	ad No 78, 2021
Division 4	
Subdivision A	
c 101.....	ad No 78, 2021
c 102.....	ad No 78, 2021
c 103.....	ad No 78, 2021
c 104.....	ad No 78, 2021
c 105.....	ad No 78, 2021
c 106.....	ad No 78, 2021
Subdivision B	
c 107.....	ad No 78, 2021
c 108.....	ad No 78, 2021
c 109.....	ad No 78, 2021
Part 5	
c 110.....	ad No 78, 2021
c 111.....	ad No 78, 2021
c 112.....	ad No 78, 2021
Part 6	
c 113.....	ad No 78, 2021
c 114.....	ad No 78, 2021
	am No 131, 2021
c 115.....	ad No 78, 2021
c 116.....	ad No 78, 2021
c 117.....	ad No 78, 2021
c 118.....	ad No 78, 2021
c 119.....	ad No 78, 2021
Part 7	
c 120.....	ad No 78, 2021

Endnote 4—Amendment history

Provision affected	How affected
c 121.....	ad No 78, 2021
c 122.....	ad No 78, 2021
Part 8	
c 123.....	ad No 78, 2021
c 124.....	ad No 78, 2021
c 125.....	ad No 78, 2021
c 126.....	ad No 78, 2021
	am No 78, 2021
Part 9	
Division 1	
c 127.....	ad No 78, 2021
Division 2	
c 128.....	ad No 78, 2021
c 129.....	ad No 78, 2021
c 130.....	ad No 78, 2021
c 131.....	ad No 78, 2021
c 132.....	ad No 78, 2021
	am No 131, 2021
Division 3	
c 133.....	ad No 78, 2021
c 134.....	ad No 78, 2021
c 135.....	ad No 78, 2021
c 136.....	ad No 78, 2021
c 137.....	ad No 78, 2021
c 138.....	ad No 78, 2021
Division 4	
c 139.....	ad No 78, 2021
	am No 131, 2021
Division 5	
c 140.....	ad No 78, 2021

Endnotes

Endnote 4—Amendment history

Provision affected	How affected
Part 10	
c 141.....	ad No 78, 2021
c 142.....	ad No 78, 2021
c 143.....	ad No 78, 2021
c 144.....	ad No 78, 2021
c 145.....	ad No 78, 2021
c 146.....	ad No 78, 2021
c 147.....	ad No 78, 2021
c 148.....	ad No 78, 2021
c 149.....	ad No 78, 2021
c 150.....	ad No 78, 2021
Part 11	
c 151.....	ad No 78, 2021
c 152.....	ad No 78, 2021
c 153.....	ad No 78, 2021
	am No 131, 2021
c 154.....	ad No 78, 2021
c 155.....	ad No 78, 2021
c 156.....	ad No 78, 2021
c 157.....	ad No 78, 2021
c 158.....	ad No 78, 2021
c 159.....	ad No 78, 2021
Part 12	
c 160.....	ad No 78, 2021
c 161.....	ad No 78, 2021
c 162.....	ad No 78, 2021
c 163.....	ad No 78, 2021
	am No 131, 2021
c 164.....	ad No 78, 2021
	am No 131, 2021
c 165.....	ad No 78, 2021

Endnote 4—Amendment history

Provision affected	How affected
	am No 131, 2021
c 166.....	ad No 78, 2021
	am No 131, 2021
Part 13	
c 167.....	ad No 78, 2021
c 168.....	ad No 78, 2021
c 169.....	ad No 78, 2021
Part 14	
c 170.....	ad No 78, 2021
c 171.....	ad No 78, 2021
c 172.....	ad No 78, 2021
c 173.....	ad No 78, 2021
c 174.....	ad No 78, 2021
c 175.....	ad No 78, 2021
c 176.....	ad No 78, 2021
c 177.....	ad No 78, 2021
	am No 131, 2021
c 178.....	ad No 78, 2021
c 179.....	ad No 78, 2021
c 180.....	ad No 78, 2021
c 181.....	ad No 78, 2021
c 182.....	ad No 78, 2021
c 183.....	ad No 78, 2021
c 184.....	ad No 78, 2021