Telecommunications (Interception and Access) Act 1979

No. 114, 1979

Compilation No. 95

Compilation date:	1 July 2017
Includes amendments up to:	Act No. 50, 2017
Registered:	3 July 2017

This compilation includes commenced amendments made by Act No. 86, 2016

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 1 July 2017 (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If a provision of the compiled law has been repealed in accordance with a provision of the law, details are included in the endnotes.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 *Criminal Code* 1
4B Application to Norfolk Island 2

Part 1-2—Interpretation 3

5 Interpretation 3
5AA Eligible Commonwealth authority declarations 45
5AB Authorised officers 45
5AC Authorisation of certifying officers 46
5AD Authorisation of certifying person 48
5AE Authorisation of members of the staff of a Commonwealth Royal Commission 48
5A Communicating etc. certain information 48
5B Exempt proceedings 48
5C Information or question relevant to inspection by Ombudsman 52
5D Serious offences 53
5E Serious contraventions 60
5EA Serious foreign contraventions 61
5F When a communication is passing over a telecommunications system 61
5G The intended recipient of a communication 61
5H When a communication is accessible to the intended recipient 62
6 Interception of a communication 62
6AAA When a computer network is appropriately used by an employee etc. of a Commonwealth agency etc. 64
6AA Accessing a stored communication 65
6A Investigation of an offence 65
6B Involvement in an offence 66
6C Issue of warrant to agency or eligible authority 66
6D Judges 66
6DA Nominated AAT members 67

Authorised Version C2017C00192 registered 03/07/2017

6DB Issuing authorities 68
6DC Part 4-1 issuing authorities 69
6E Lawfully intercepted information 70
6EA Interception warrant information 70
6EAA Preservation notice information 71
6EB Stored communications warrant information 71
6F Offences 72
6G Officer of the Commonwealth, of a State or of a Territory 72
6H Person to whom application relates 73
6J Proceeding by way of a prosecution for an offence 73
6K Proceeding for confiscation or forfeiture or for pecuniary penalty 73
6L Relevant proceeding 74
6M Terminating the appointment of an officer 77
6N Declaration of staff members of State Police Forces 77
6P Identification of service 77
6Q Identification of telecommunications device 77
6R Communications Access Co-ordinator 78
6S Permitted purposes—integrity purposes 78
6T When control order is taken to be in force 80
6U Succeeding control orders 80

Chapter 2—Interception of telecommunications 81

Part 2-1—Prohibition on interception of telecommunications 81
7 Telecommunications not to be intercepted 81

Part 2-2—Warrants authorising the Organisation to intercept telecommunications 86
9 Issue of telecommunications service warrants by Attorney-General 86
9A Issue of named person warrants by Attorney-General 87
9B Provisions applying to warrants issued under section 9 or 9A 90
10 Issue of warrant by Director-General of Security in emergency for Organisation to intercept telecommunications 91
11A Telecommunications service warrant for collection of foreign intelligence 92
11B Named person warrant for collection of foreign intelligence 93
11C Foreign communications warrant for collection of foreign intelligence 96
11D Provisions applying to foreign intelligence warrants 97

Authorised Version C2017C00192 registered 03/07/2017

12 Persons authorised to intercept communications for Organisation 99
13 Discontinuance of interception before expiration of warrant 99
14 Certain records retained by Organisation to be destroyed 99
15 How warrants etc. to be dealt with 100
16 Additional requirements for named person warrants 102
17 Reports to be made to Attorney-General on results of interception 104
18 Evidentiary certificates 104

Part 2-3—Emergency requests authorising officers of a carrier to intercept telecommunications 106
30 Emergency requests 106

Part 2-4—Authorisation of interception for developing and testing interception capabilities 108
31 Applications for authorisation 108
31A Attorney-General may authorise interception for developing and testing interception capabilities 109
31B Authorisation of employees of a security authority 109
31C Destruction of records 110
31D Reports to the Attorney-General 110

Part 2-5—Warrants authorising agencies to intercept telecommunications 111

Division 2—Declaration of State Law Enforcement Authorities as Agencies 111
34 Declaration of an eligible authority of a State as an agency 111
35 Preconditions for declaration 111
36 State laws requiring copies of documents to be given to responsible Minister 114
37 Revocation of declaration 114
38 Effect of revocation 115
38A Agencies authorised to apply for control order warrants 115

Division 3—Applications for warrants 118
39 Agency may apply for warrant 118
40 Form of application 119
41 Contents of application 120
42 Affidavit to accompany written application 120
43 Information to be given on telephone application 121

Authorised Version C2017C00192 registered 03/07/2017

44 Giving further information to Judge 122
44A Application by interception agency of Victoria 122
45 Application by interception agency of Queensland 123
45A State law not affected 124

Division 4—Warrants 125

46 Issue of telecommunications service warrant 125
46A Issue of named person warrant 131
47 Limit on authority conferred by warrant 137
48 Issue of warrant for entry on premises 137
49 Form and content of warrant 139
50 Issue of warrant on telephone application 141
51 Action by agency after warrant issued on telephone application 141
52 Judge or nominated AAT member may revoke warrant where section 51 contravened 142
54 Entry into force of warrants 143
55 Exercise of authority conferred by warrant 143
57 Revocation of warrant by chief officer 144
58 Discontinuance of interceptions under certain warrants 145
59 When revocation of certain warrants takes effect 145
59A Notification to Secretary of the Department 145
59B Notification to Ombudsman by Commonwealth agencies in relation to control order warrants 146
60 Notification to authorised representative of carrier of issue or revocation of certain warrants 147
61 Evidentiary certificates 149
61A Certified copy of warrant 151

Part 2-6—Dealing with intercepted information etc. 152

62 Application of Part 152
63 No dealing in intercepted information or interception warrant information 152
63AA Dealing in interception warrant information for the purposes of Part 2-2, 2-5, 2-7 or 2-8 153
63A Dealing in connection with existing proceeding 153
63B Dealing in information by employees of carriers 154
63C Dealing in information for network protection purposes etc. 155
63D Dealing in information for disciplinary purposes 155
63E Responsible person for a computer network may communicate information to an agency 156

Authorised Version C2017C00192 registered 03/07/2017

64 Dealing in connection with Organisation's or Inspector-General's functions 157
65 Communicating information obtained by Organisation 158
65A Employee of carrier may communicate information to agency 159
66 Interceptor may communicate to officer who applied for warrant or authorised person 159
67 Dealing for permitted purpose in relation to agency 160
68 Chief officer may communicate information obtained by agency 162
68A Communicating information obtained by Secretary 166
69 State authority may ask not to receive information under section 68 166
70 Communicating information obtained by interception under Part 2-3 167
71 Dealing with information where interception suspected to be unlawful 167
72 Making record for purpose of permitted communication 168
73 Further dealing by recipient of certain information 168
74 Giving information in evidence in exempt proceeding 169
75 Giving information in evidence where defect in connection with warrant 169
75A Evidence that has been given in exempt proceeding 170
76 Giving information in evidence in criminal proceedings under this Act 170
76A Giving information in evidence in civil proceedings for remedial relief 171
77 Intercepted material and interception warrant information inadmissible except as provided 171
78 Where evidence otherwise inadmissible 172
79 Destruction of restricted records that are not likely to be required for a permitted purpose 173
79AA Destruction of restricted records—information obtained before a control order came into force 173
79A Responsible person for a computer network must ensure restricted records are destroyed 174

Part 2-7—Keeping and inspection of interception records 176

80 Commonwealth agencies to keep documents connected with issue of warrants 176
81 Other records to be kept by Commonwealth agencies in connection with interceptions 176

Authorised Version C2017C00192 registered 03/07/2017

81AA Organisation to record particulars in relation to eligible authorities of a State 178
81A General Register of Warrants 179
81B Regular submission of General Register to Minister 180
81C Special Register of Warrants 180
81D Regular submission of Special Register to Minister 183
81E Provision of information by eligible authorities 183
83 Inspections 184
84 Reports 184
85 Ombudsman may report on other breaches of this Act 185
85A Annual report may cover notified breaches in relation to control order warrants 186
86 Ombudsman's general powers 186
87 Power to obtain relevant information 187
88 Ombudsman to be given information and access notwithstanding other laws 188
89 Dealing with information for the purposes of inspection and report 189
90 Ombudsman not to be sued 190
91 Delegation by Ombudsman 190
92 Application of Ombudsman Act 190
92A Exchange of information between Ombudsman and State inspecting authorities 191

Part 2-8—Reports about interceptions under Parts 2-3 and 2-5 193

Division 1—Reports to the Minister 193

93 Annual reports to Minister about interceptions under Part 2-3 193
94 Annual reports regarding applications and warrants under Part 2-5 193
94A Reports regarding emergency interception action 194
94B Reports regarding named person warrants 195
95 Minister may seek further information from Commonwealth agency 196
96 Annual reports by State authorities 196
97 Reports by Managing Directors about acts done in connection with certain warrants under Part 2-5 197

Division 2—Reports by the Minister 198

99 Annual report by Minister about warrants under Part 2-5 198
100 Report to set out how many applications made and warrants issued 198

Authorised Version C2017C00192 registered 03/07/2017

101 Report to contain particulars about duration of warrants 201
102 Report to contain information about effectiveness of warrants 203
102A Report regarding interceptions without warrant 206
102B Report regarding mutual assistance requests 206
103 Other information to be included in report 206
103A Annual report for 1999-2000 208
103B Deferral of inclusion of information in report 208

Division 3—Provisions about annual reports 211
104 Annual reports 211

Part 2-9—Offences 212
105 Contravention of section 7 or 63 212
106 Obstruction 212
107 Offences relating to inspections under Part 2-7 213

Part 2-10—Civil remedies 214
107A Civil remedies—unlawful interception or communication 214
107B Limitation periods etc. 217
107C No limitation on other liability 217
107D Concurrent operation of State and Territory laws 218
107E State or Territory courts—jurisdictional limits 218
107F Extended meaning of *conviction*—orders under section 19B of the *Crimes Act 1914* 218

Chapter 3—Preserving and accessing stored communications 219

Part 3-1A—Preserving stored communications 219

Division 1—Outline of this Part 219
107G Outline of this Part 219

Division 2—Domestic preservation notices 221
107H Domestic preservation notices 221
107J Conditions for giving domestic preservation notices 221
107K When a domestic preservation notice is in force 223
107L Revoking a domestic preservation notice 223
107M Persons who act on the issuing agency's behalf 224

Division 3—Foreign preservation notices 226
107N When a foreign preservation notice can be given 226

Authorised Version C2017C00192 registered 03/07/2017

107P Condition for giving a foreign preservation notice 226
107Q When a foreign preservation notice is in force 227
107R Revoking a foreign preservation notice 228
107S Persons who act on the AFP's behalf 229

Division 4—Provisions relating to preservation notices 230
107T Evidentiary certificates relating to actions by carriers 230
107U Evidentiary certificates relating to actions by issuing agencies 230
107V Certified copies of preservation notices 231
107W How notices are to be given to carriers 231

Part 3-1—Prohibition on access to stored communications 232
108 Stored communications not to be accessed 232

Part 3-2—Access by the Organisation to stored communications 235
109 Access to stored communications under Part 2-2 warrants 235

Part 3-3—Access by criminal law-enforcement agencies to stored communications 236

Division 1—Applications for warrants 236
110 Criminal law-enforcement agencies may apply for stored communications warrants 236
110A Meaning of *criminal law-enforcement agency* 236
110B Declarations in relation to the Immigration and Border Protection Department 240
111 Form of applications 241
112 Contents of written applications 241
113 Affidavits to accompany written applications 241
114 Information to be given on telephone applications 242
115 Giving further information to Judge 242

Division 2—Issuing of warrants 243
116 Issuing of stored communications warrants 243
117 What stored communications warrants authorise 245
118 Form and content of stored communications warrants 245
119 Duration of stored communications warrants 246

Division 3—How warrants etc. are dealt with 247
120 Stored communications warrants issued on telephone applications 247

Authorised Version C2017C00192 registered 03/07/2017

121 What happens when stored communications warrants are issued 248
122 Revocation of stored communications warrants by chief officers 248
123 What happens when stored communications warrants are revoked 249
124 Access to additional telecommunications services under stored communications warrants 249

Division 4—Provisions relating to execution of warrants 251

125 Entry into force of stored communications warrants 251
126 Limit on authority conferred by warrant 251
127 Exercise of authority conferred by warrant 251
128 Provision of technical assistance 252
129 Evidentiary certificates relating to actions by carriers 252
130 Evidentiary certificates relating to actions by criminal law-enforcement agencies 253
131 Certified copies of stored communications warrants 254
132 Obstruction 254

Part 3-4—Dealing with accessed information etc. 255

Division 1—Prohibition on dealing with accessed information etc. 255

133 No dealing with accessed information etc. 255

Division 2—Permitted dealings with accessed information 256

134 Dealing in preservation notice information or stored communications warrant information 256
135 Dealing in information by employees of carriers 256
136 Dealing in connection with Organisation's functions 258
137 Communicating information obtained by Organisation 259
138 Employee of carrier may communicate information to criminal law-enforcement agency 260
139 Dealing for purposes of investigation etc. 260
139A Dealing for integrity purposes 262
139B Dealing for purposes relating to control orders and preventative detention orders 263
139C Dealing for purposes relating to continuing detention orders 263
140 Dealing with information if access suspected to be unlawful 264
141 Making record for purpose of permitted communication 265
142 Further dealing by recipient of certain information 265

Authorised Version C2017C00192 registered 03/07/2017

142A Communicating information obtained as a result of a mutual assistance application to foreign country 265
143 Giving information in evidence in exempt proceeding 266
144 Giving information in evidence if communication unlawfully accessed 266
145 Evidence that has been given in exempt proceeding 267
146 Giving information in evidence in civil proceedings for remedial relief 267

Division 3—Admissibility of evidence 268
147 Accessed material inadmissible except as provided 268
148 Stored communications warrant information inadmissible except as provided 268
149 Evidence that is otherwise inadmissible 269

Division 4—Destruction of records 270
150 Destruction of records 270

Part 3-5—Keeping and inspection of records 271

Division 1—Obligation to keep records 271
151 Obligation to keep records 271

Division 3—Inspection of preservation notice records by Inspector-General of Intelligence and Security 273
158A Functions of the Inspector-General of Intelligence and Security 273

Part 3-6—Reports about access to stored communications 274

Division 1—Reports to the Minister 274
159 Annual reports regarding applications and warrants under Part 3-3 274
160 Minister may seek further information from Commonwealth agency 274

Division 2—Reports by the Minister 275
161 Annual report by Minister about stored communications warrants 275
161A Report to contain information about preservation notices 275
162 Report to set out how many applications made and warrants issued 275
163 Report to contain information about effectiveness of warrants 277
163A Report regarding mutual assistance requests 277

Authorised Version C2017C00192 registered 03/07/2017

Division 3—Provisions about annual reports 278
164 Annual reports 278

Part 3-7—Civil remedies 279
165 Civil remedies—unlawful access or communication 279
166 Limitation periods etc. 282
167 No limitation on other liability 282
168 Concurrent operation of State and Territory laws 283
169 State or Territory courts—jurisdictional limits 283
170 Extended meaning of *conviction*—orders under section 19B of the *Crimes Act 1914* 283

Chapter 4—Access to telecommunications data 284

Part 4-1—Permitted access to telecommunications data 284

Division 1—Outline of Part 284
171 Outline of Part 284

Division 2—General provisions 285
172 No disclosure of the contents or substance of a communication 285
173 Effect of Divisions 3 to 5 285

Division 3—The Organisation 286
174 Voluntary disclosure 286
175 Authorisations for access to existing information or documents 286
176 Authorisations for access to prospective information or documents 287

Division 4—Enforcement agencies 289
176A Meaning of *enforcement agency* 289
177 Voluntary disclosure 291
178 Authorisations for access to existing information or documents—enforcement of the criminal law 292
178A Authorisations for access to existing information or documents—locating missing persons 293
179 Authorisations for access to existing information or documents—enforcement of a law imposing a pecuniary penalty or protection of the public revenue 293
180 Authorisations for access to prospective information or documents 294

Authorised Version C2017C00192 registered 03/07/2017

Division 4A—Foreign law enforcement 296

Subdivision A—Primary disclosures 296

180A Authorisations for access to existing information or documents—enforcement of the criminal law of a foreign country 296

180B Authorisations for access to prospective information or documents—enforcement of the criminal law of a foreign country 297

Subdivision B—Secondary disclosures 299

180C Authorisations to disclose information or documents—enforcement of the criminal law of a foreign country 299

180D Authorisations to disclose information or documents—enforcement of the criminal law 300

Subdivision C—Conditions of disclosure to foreign country 301

180E Disclosing information etc. obtained to foreign country 301

Division 4B—Privacy to be considered when making authorisations 302

180F Authorised officers to consider privacy 302

Division 4C—Journalist information warrants 303

Subdivision A—The requirement for journalist information warrants 303

180G The Organisation 303

180H Enforcement agencies 303

Subdivision B—Issuing journalist information warrants to the Organisation 304

180J Requesting a journalist information warrant 304

180K Further information 305

180L Issuing a journalist information warrant 305

180M Issuing a journalist information warrant in an emergency 306

180N Duration of a journalist information warrant 308

180P Discontinuance of authorisations before expiry of a journalist information warrant 308

Subdivision C—Issuing journalist information warrants to enforcement agencies 309

180Q Enforcement agency may apply for a journalist information warrant 309

180R Further information 310

180S Oaths and affirmations 310

Authorised Version C2017C00192 registered 03/07/2017

180T Issuing a journalist information warrant 310
180U Form and content of a journalist information warrant 312
180V Entry into force of a journalist information warrant 312
180W Revocation of a journalist information warrant by chief officer 312

Subdivision D—Miscellaneous 313
180X Public Interest Advocates 313

Division 5—Uses of telecommunications data connected with provision of access 314
181 Uses of telecommunications data connected with provision of access 314

Division 6—Disclosure/use offences 315
181A Disclosure/use offences: authorisations under Division 3 315
181B Disclosure/use offences: certain authorisations under Division 4 317
182 Secondary disclosure/use offence: disclosures under Division 4 319
182A Disclosure/use offences: journalist information warrants 322
182B Permitted disclosure or use: journalist information warrants 323

Part 4-2—Procedural requirements relating to authorisations 324
183 Form of authorisations and notifications 324
184 Notification of authorisations or revocations 324
185 Retention of authorisations 325
185A Evidentiary certificates relating to acts by carriers 326
185B Evidentiary certificates relating to acts by the Organisation 327
185C Evidentiary certificates relating to acts by enforcement agencies 327
185D Notification etc. of authorisations intended to identify media sources 328
185E Reports on access to retained data 330
186 Report to Minister 331
186A Obligation to keep records 334

Chapter 4A—Oversight by the Commonwealth Ombudsman 338
186B Inspection of records 338
186C Power to obtain relevant information 339
186D Ombudsman to be given information and access despite other laws 340

Authorised Version C2017C00192 registered 03/07/2017

186E Application of Ombudsman Act 341
186F Exchange of information between Ombudsman and State inspecting authorities 342
186G Delegation by Ombudsman 342
186H Ombudsman not to be sued 343
186J Reports 343

Chapter 5—Co-operation with agencies 345

Part 5-1—Definitions 345
187 Definitions 345

Part 5-1A—Data retention 346

Division 1—Obligation to keep information and documents 346
187A Service providers must keep certain information and documents 346
187AA Information to be kept 349
187B Certain service providers not covered by this Part 352
187BA Ensuring the confidentiality of information 353
187C Period for keeping information and documents 353

Division 2—Data retention implementation plans 355
187D Effect of data retention implementation plans 355
187E Applying for approval of data retention implementation plans 355
187F Approval of data retention implementation plans 356
187G Consultation with agencies and the ACMA 357
187H When data retention implementation plans are in force 359
187J Amending data retention implementation plans 359

Division 3—Exemptions 361
187K The Communications Access Co-ordinator may grant exemptions or variations 361
187KA Review of exemption or variation decisions 363

Division 4—Miscellaneous 365
187KB Commonwealth may make a grant of financial assistance to service providers 365
187L Confidentiality of applications 365
187LA Application of the *Privacy Act 1988* 366
187M Pecuniary penalties and infringement notices 366
187N Review of operation of Part 366
187P Annual reports 367

Authorised Version C2017C00192 registered 03/07/2017

Part 5-2—Delivery points 369
188 Delivery points 369

Part 5-3—Interception capability 372

Division 1—Obligations 372
189 Minister may make determinations 372
190 Obligations of persons covered by a determination 373
191 Obligations of persons not covered by a determination in relation to a kind of telecommunications service 373

Division 2—Exemptions 375
192 The Communications Access Co-ordinator may grant exemptions 375
193 ACMA may grant exemptions for trial services 376

Part 5-4—Interception capability plans 377
195 Nature of an interception capability plan 377
196 Time for giving IC plans by carriers 378
197 Time for giving IC plans by nominated carriage service providers 378
198 Consideration of IC plans 379
199 Commencement of IC plans 381
200 Compliance with IC plans 382
201 Consequences of changed business plans 382
202 Confidential treatment of IC plans 382

Part 5-4A—Requirement arising from proposed changes 384
202A Purpose of Part 384
202B Carrier or provider to notify of proposed change 384
202C Communications Access Co-ordinator may notify agencies 386

Part 5-5—Delivery capability 387
203 Communications Access Co-ordinator may make determinations 387
204 Obligations of persons covered by a determination 388
205 Obligations of persons not covered by a determination in relation to a kind of telecommunications service 388

Part 5-6—Allocation of costs 389

Division 1—Outline of Part 389
206 Outline of Part 389

Authorised Version C2017C00192 registered 03/07/2017

Division 2—Interception capability 390
207 Costs to be borne by the carriers....390
Division 3—Delivery capability 391
208 Costs to be borne by the interception agencies....391
209 Working out costs of delivery capabilities....391
210 Examination of lower cost options....393
211 ACMA may require independent audit of costs....393
Chapter 6—Miscellaneous 395
Part 6-1—Miscellaneous 395
298 Protection of persons—control order declared to be void....395
299 Dealing with information obtained under a warrant—control order declared to be void....395
300 Regulations....396
Endnotes 398
Endnote 1—About the endnotes 398
Endnote 2—Abbreviation key 400
Endnote 3—Legislation history 401
Endnote 4—Amendment history 422

Authorised Version C2017C00192 registered 03/07/2017

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 related 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.

Authorised Version C2017C00192 registered 03/07/2017

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*.

Authorised Version C2017C00192 registered 03/07/2017

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.

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

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

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*.

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:

(a) aiding, abetting, counselling or procuring the commission of an offence;

Authorised Version C2017C00192 registered 03/07/2017

(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.

ASIO affiliate has the same meaning as in 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:

Authorised Version C2017C00192 registered 03/07/2017

(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:
(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:

Authorised Version C2017C00192 registered 03/07/2017

(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

Authorised Version C2017C00192 registered 03/07/2017

(e) in the case of the Independent Commission Against Corruption:
  (i) the 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

(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

Authorised Version C2017C00192 registered 03/07/2017

(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

Authorised Version C2017C00192 registered 03/07/2017

(e) in the case of the Independent Commission Against Corruption—the 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

(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.

Authorised Version C2017C00192 registered 03/07/2017

Section 5

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*.

Authorised Version C2017C00192 registered 03/07/2017

control order warrant means a warrant issued:

(a) under subsection 46(4) or 46A(2A); or

(b) under section 48 in the circumstances mentioned in subsection 46(4).

control order 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 control order warrants (see section 38A).

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

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.

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

Authorised Version C2017C00192 registered 03/07/2017

(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.

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.

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

Authorised Version C2017C00192 registered 03/07/2017

(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.

examiner has the same meaning as in the ACC Act.

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

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

Authorised Version C2017C00192 registered 03/07/2017

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.

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

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

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.

Authorised Version C2017C00192 registered 03/07/2017

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

Authorised Version C2017C00192 registered 03/07/2017

(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

(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, has the meaning given by section 5G.

interception agency means:

(a) except for the purposes of section 6R, Part 2-6 or Chapter 5:

Authorised Version C2017C00192 registered 03/07/2017

(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*.

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 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).

Authorised Version C2017C00192 registered 03/07/2017

lawfully accessed information means information obtained by accessing a stored communication otherwise than in contravention of subsection 108(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.

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.

Authorised Version C2017C00192 registered 03/07/2017

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 (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)).

Authorised Version C2017C00192 registered 03/07/2017

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.

mutual assistance application means an application for a stored communications warrant made as a result of an authorisation under section 15B of the *Mutual Assistance in Criminal Matters Act 1987*.

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

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 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).

Authorised Version C2017C00192 registered 03/07/2017

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

(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

Authorised Version C2017C00192 registered 03/07/2017

(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

Authorised Version C2017C00192 registered 03/07/2017

(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).

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.

Authorised Version C2017C00192 registered 03/07/2017

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.

passing over includes being carried.

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 or an eligible authority of a State, means a purpose connected with:

(a) in any case (except in the case of the Immigration and Border Protection Department):

Authorised Version C2017C00192 registered 03/07/2017

(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) an 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

Authorised Version C2017C00192 registered 03/07/2017

(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

(iii) 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 of the *Criminal Code*; or

(vi) a preventative detention order law; or

(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, Division 105A of the *Criminal Code*, so far as the function, duty or power relates to a continuing detention order or an interim detention order; or

Authorised Version C2017C00192 registered 03/07/2017

(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

(ba) 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

(iia) 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

(iib) 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

(iva) 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 105A of the *Criminal Code*, so far as the function, duty or power relates to a continuing detention order or an interim detention order; or

Authorised Version C2017C00192 registered 03/07/2017

(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 of the *Criminal Code* (Control orders); or

(vii) a preventative detention order law; 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:

(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

Authorised Version C2017C00192 registered 03/07/2017

(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:

Authorised Version C2017C00192 registered 03/07/2017

(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 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.

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

Authorised Version C2017C00192 registered 03/07/2017

(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.

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.

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 an 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

Authorised Version C2017C00192 registered 03/07/2017

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

Authorised Version C2017C00192 registered 03/07/2017

(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.

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.

Authorised Version C2017C00192 registered 03/07/2017

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.

Authorised Version C2017C00192 registered 03/07/2017

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

record 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.

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:

Authorised Version C2017C00192 registered 03/07/2017

(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

Authorised Version C2017C00192 registered 03/07/2017

(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

(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, means all of the following:

(a) how many applications of that kind were made;

Authorised Version C2017C00192 registered 03/07/2017

(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.

Authorised Version C2017C00192 registered 03/07/2017

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.

serious offence has the meaning given by section 5D.

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.

Authorised Version C2017C00192 registered 03/07/2017

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*.

State includes the Northern Territory.

stored communication 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 control order has the meaning given by section 6U.

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

Authorised Version C2017C00192 registered 03/07/2017

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.

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 means an application made by telephone for a Part 2-5 warrant or a stored communications warrant.

Authorised Version C2017C00192 registered 03/07/2017

Territory does not include the Northern Territory.

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

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).

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); 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*.

Authorised Version C2017C00192 registered 03/07/2017

(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

Authorised Version C2017C00192 registered 03/07/2017

(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.

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:

Authorised Version C2017C00192 registered 03/07/2017

(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:

Authorised Version C2017C00192 registered 03/07/2017

(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.

(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 Commissioner of the Independent Commission Against Corruption may authorise, in writing, an officer of the Independent

Authorised Version C2017C00192 registered 03/07/2017

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

(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

Authorised Version C2017C00192 registered 03/07/2017

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.

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, 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

Authorised Version C2017C00192 registered 03/07/2017

(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 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

(bd) a proceeding under, or a proceeding relating to a matter arising under, Division 105A of the *Criminal Code*, so far as the proceeding relates to a continuing detention order or an interim detention order; 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

Authorised Version C2017C00192 registered 03/07/2017

(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 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

Authorised Version C2017C00192 registered 03/07/2017

(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

(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

Authorised Version C2017C00192 registered 03/07/2017

(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

(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.

Authorised Version C2017C00192 registered 03/07/2017

(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
    (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
    (vi) Division 119 of the *Criminal Code*; or
  (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 a 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

Authorised Version C2017C00192 registered 03/07/2017

(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;

Authorised Version C2017C00192 registered 03/07/2017

(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 270.8 (slavery or slavery-like conditions);
(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);
(v) section 271.7F or 271.7G (harbouring victims);
(vi) section 271.8 or 271.9 (debt bondage); or
(b) section 233A, 233B, 233C, 233D, 233E, 234 or 234A of the *Migration Act 1958*.

Sexual offences against children and offences involving child pornography or harm to children

(3B) An offence is also a serious offence if:
(a) it is an offence against Division 272 or 273, Subdivision B or C of Division 471, or Subdivision D or F of Division 474, of the *Criminal Code*; or

Authorised Version C2017C00192 registered 03/07/2017

(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 pornography; or
(ii) consenting to or procuring the employment of a child, or employing a child, in connection with child pornography.

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);
(aa) section 135.3 of the *Criminal Code*;
(b) Division 1A of Part IV 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*;

Authorised Version C2017C00192 registered 03/07/2017

(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
(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.

Authorised Version C2017C00192 registered 03/07/2017

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) subsection 1041G(1);
(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*;

Authorised Version C2017C00192 registered 03/07/2017

(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

(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.

Authorised Version C2017C00192 registered 03/07/2017

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

Authorised Version C2017C00192 registered 03/07/2017

that is equivalent, under section 4AA of the *Crimes Act 1914*, to that number of penalty units.

5EA Serious foreign contraventions

For the purposes of this Act, a ***serious foreign contravention*** is a contravention of a law of a foreign country that is punishable by a maximum penalty of:

(a) imprisonment for 3 years or more, imprisonment for life or the death penalty; or

(b) a fine of an amount that is at least equivalent to 900 penalty units.

5F When a communication is passing over a telecommunications system

For the purposes of this Act, 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, 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.

Authorised Version C2017C00192 registered 03/07/2017

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, 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

Authorised Version C2017C00192 registered 03/07/2017

(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 267 of the *Radiocommunications Act 1992* is lawfully engaged in performing spectrum management functions of the Australian Communications and Media Authority under the *Australian Communications*

Authorised Version C2017C00192 registered 03/07/2017

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.

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:

Authorised Version C2017C00192 registered 03/07/2017

(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.

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;

Authorised Version C2017C00192 registered 03/07/2017

(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;
(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 means a Judge in relation to whom a consent under subsection (2) and a declaration under subsection (3) are in force.

Authorised Version C2017C00192 registered 03/07/2017

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 Minister under subsection (3).

(3) The Minister 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.

(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, 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 Minister 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 or 3-3:

(a) Deputy President;

(b) senior member (of any level);

(c) member (of any level).

(2) Despite subsection (1), the Minister 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 Minister, 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 or 3-3, the same

Authorised Version C2017C00192 registered 03/07/2017

protection and immunity as a Justice of the High Court has in relation to proceedings in the High Court.

6DB Issuing authorities

(1) The Minister may, by writing, appoint as an 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, 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 Minister under subsection (1).

(3) A person's appointment ceases to have effect if:

(a) the person ceases to be a person whom the Minister could appoint under this section; or

(b) the Minister, by writing, revokes the appointment.

(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, the same protection and immunity as a Justice of the High Court has in relation to proceedings in the High Court.

Authorised Version C2017C00192 registered 03/07/2017

6DC Part 4-1 issuing authorities

(1) The Minister 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 Minister under subsection (1).

(3) A person's appointment ceases to have effect if:

(a) the person ceases to be a person whom the Minister could appoint under this section; or

(b) the Minister, 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.

Authorised Version C2017C00192 registered 03/07/2017

6E Lawfully intercepted information

(1) Subject to subsection (2), 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.

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

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

Authorised Version C2017C00192 registered 03/07/2017

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.

Authorised Version C2017C00192 registered 03/07/2017

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

(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:

Authorised Version C2017C00192 registered 03/07/2017

(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) or 46(4)(c), (d) and (e), 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), 46A(1)(c) and (d) or 46A(2A)(c), (d) and (e), 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

Authorised Version C2017C00192 registered 03/07/2017

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

(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

(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

Authorised Version C2017C00192 registered 03/07/2017

(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 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

Authorised Version C2017C00192 registered 03/07/2017

with the commission of a prescribed offence to which a prescribed investigation relates or related; or

(b) in the case of the Crime Commission, 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 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:

Authorised Version C2017C00192 registered 03/07/2017

(i) that is an offence against the law of South Australia; and
(ii) to which a prescribed investigation relates or related.

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

Authorised Version C2017C00192 registered 03/07/2017

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 (c) Australian Commission for Law Enforcement Integrity; or (d) Immigration and Border	A purpose connected with: (a) a decision about whether to apply for an integrity authority; or (b) designing, but not conducting, an integrity operation; or (c) an application for an integrity authority; or

Authorised Version C2017C00192 registered 03/07/2017

Permitted purposes—integrity purposes		
Item	**Column 1—Commonwealth agency or Immigration and Border Protection Department**	**Column 2—Permitted purpose**
	Protection Department.	(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;

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

Authorised Version C2017C00192 registered 03/07/2017

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 control order is taken to be in force

For the purposes of this Act, if:

(a) a control order has been made in relation to a person; and

(b) apart from this section, the control order has not come into force because it has not been served on the person;

the control order is taken to be in force.

6U Succeeding control orders

If 2 or more successive control orders are made in relation to the same person, each later control order is a ***succeeding control order*** in relation to each earlier control order.

Authorised Version C2017C00192 registered 03/07/2017

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

Authorised Version C2017C00192 registered 03/07/2017

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

(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.

Authorised Version C2017C00192 registered 03/07/2017

(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:

Authorised Version C2017C00192 registered 03/07/2017

(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:

(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.

Authorised Version C2017C00192 registered 03/07/2017

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 control 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.

Authorised Version C2017C00192 registered 03/07/2017

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.

Authorised Version C2017C00192 registered 03/07/2017

(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:

Authorised Version C2017C00192 registered 03/07/2017

(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.

Authorised Version C2017C00192 registered 03/07/2017

(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.

Authorised Version C2017C00192 registered 03/07/2017

Section 9B

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.

Authorised Version C2017C00192 registered 03/07/2017

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

Authorised Version C2017C00192 registered 03/07/2017

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

Authorised Version C2017C00192 registered 03/07/2017

(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.

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:

Authorised Version C2017C00192 registered 03/07/2017

(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:

(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.

Authorised Version C2017C00192 registered 03/07/2017

(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.

Authorised Version C2017C00192 registered 03/07/2017

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

(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 foreign communications 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 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 foreign communications in order to collect the intelligence referred to in paragraph (a); 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 foreign communications for the purpose of obtaining that intelligence.

(2) A warrant under subsection (1) must not authorise the interception of any communications except foreign communications.

Authorised Version C2017C00192 registered 03/07/2017

(3) A request by the Director-General of Security for the issue of a warrant under this section must:

(a) include a description that is sufficient to identify the part of the telecommunications system that is likely to carry the foreign communications whose interception is sought; 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.

(4) A warrant under this section must include:

(a) a notice addressed to the carrier who operates the relevant telecommunications system, giving a description that is sufficient to identify the part of the telecommunications system that is covered by the warrant; and

(b) a notice addressed to the Director-General of Security stating that the warrant authorises the obtaining of foreign intelligence only for purposes relating to the matter specified in the notice requesting the issue of the warrant.

(5) Where:

(a) a communication is intercepted under a warrant under this section; and

(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 cause any record or copy of the communication to be destroyed.

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:

Authorised Version C2017C00192 registered 03/07/2017

(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

(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.

(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:

Authorised Version C2017C00192 registered 03/07/2017

(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

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 as persons authorized to exercise, on behalf of the Organisation, the authority conferred by Part 2-2 warrants.

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.

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.

Authorised Version C2017C00192 registered 03/07/2017

Note: See subsection 11C(5) 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

Authorised Version C2017C00192 registered 03/07/2017

(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

(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;

Authorised Version C2017C00192 registered 03/07/2017

(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;

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) where, under paragraph (1)(b), the Director-General of Security receives the warrant—a copy of the part of the warrant referred to in paragraph 11C(4)(a), 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.

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;

Authorised Version C2017C00192 registered 03/07/2017

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 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.

Authorised Version C2017C00192 registered 03/07/2017

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

Authorised Version C2017C00192 registered 03/07/2017

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 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*.

Authorised Version C2017C00192 registered 03/07/2017

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).

Authorised Version C2017C00192 registered 03/07/2017

(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.

Authorised Version C2017C00192 registered 03/07/2017

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 by employees of the 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
  (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.

Authorised Version C2017C00192 registered 03/07/2017

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

(5) An authorisation given under subsection (1) is not a legislative instrument.

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.

Authorised Version C2017C00192 registered 03/07/2017

(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 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.

Authorised Version C2017C00192 registered 03/07/2017

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 control order 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

Authorised Version C2017C00192 registered 03/07/2017

(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

Authorised Version C2017C00192 registered 03/07/2017

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.

Authorised Version C2017C00192 registered 03/07/2017

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

Authorised Version C2017C00192 registered 03/07/2017

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 control order 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 control order 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 control order 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).

Authorised Version C2017C00192 registered 03/07/2017

Criteria to be authorised to apply for a control order 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 control order 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 control order warrants if the Minister is satisfied that:

Authorised Version C2017C00192 registered 03/07/2017

(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 control order warrants.

(7) If the Minister amends the declaration under subsection (5) or (6), the amendment does not affect the validity of a control order warrant issued before the amendment in response to an application by the eligible authority.

Authorised Version C2017C00192 registered 03/07/2017

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

Authorised Version C2017C00192 registered 03/07/2017

(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.

Authorised Version C2017C00192 registered 03/07/2017

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

Authorised Version C2017C00192 registered 03/07/2017

(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.

Authorised Version C2017C00192 registered 03/07/2017

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) or 46(5)(a) to (f), 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) or 46A(2B)(a) to (f), as the case requires.

PIM may question certain persons

(3) The Victorian 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

Authorised Version C2017C00192 registered 03/07/2017

(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) or 46(5)(a) to (f), 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) or 46A(2B)(a) to (f), 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.

Authorised Version C2017C00192 registered 03/07/2017

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.

Authorised Version C2017C00192 registered 03/07/2017

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.

Authorised Version C2017C00192 registered 03/07/2017

(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

Authorised Version C2017C00192 registered 03/07/2017

(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.

Control order warrant

(4) If a control order 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 control order is in force in relation to the particular person; or

(ii) a control 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) the protection of the public from a terrorist act; or

(ii) preventing the provision of support for, or the facilitation of, a terrorist act; or

(iii) preventing the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country; or

Authorised Version C2017C00192 registered 03/07/2017

(iv) determining whether the control order, or any succeeding control 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 control 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) the protection of the public from a terrorist act; or

(ii) preventing the provision of support for, or the facilitation of, a terrorist act; or

(iii) preventing the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country; or

(iv) determining whether the control order, or any succeeding control order, has been, or is being, complied with; and

(c) to what extent methods for:

(i) the protection of the public from a terrorist act; or

(ii) preventing the provision of support for, or the facilitation of, a terrorist act; or

Authorised Version C2017C00192 registered 03/07/2017

(iii) preventing the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country; or

(iv) determining whether the control order, or any succeeding control 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) the protection of the public from a terrorist act; or

(ii) preventing the provision of support for, or the facilitation of, a terrorist act; or

(iii) preventing the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country; or

(iv) determining whether the control order, or any succeeding control order, has been, or is being, complied with; and

(e) how much the use of such methods would be likely to prejudice:

(i) the protection of the public from a terrorist act; or

(ii) preventing the provision of support for, or the facilitation of, a terrorist act; or

(iii) preventing the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country; or

(iv) determining whether the control order, or any succeeding control 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

Authorised Version C2017C00192 registered 03/07/2017

(g) 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; or

(vi) has contravened, is contravening, or will contravene, the control order; or

(vii) will contravene a succeeding control 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 control 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.

Authorised Version C2017C00192 registered 03/07/2017

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;

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.

Authorised Version C2017C00192 registered 03/07/2017

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

Authorised Version C2017C00192 registered 03/07/2017

(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.

Control order warrant

(2A) If a control order 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 control 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

(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) the protection of the public from a terrorist act; or

(iv) preventing the provision of support for, or the facilitation of, a terrorist act; or

Authorised Version C2017C00192 registered 03/07/2017

(v) preventing the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country; or

(vi) determining whether the control order, or any succeeding control 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 control 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) the protection of the public from a terrorist act; or

(ii) preventing the provision of support for, or the facilitation of, a terrorist act; or

Authorised Version C2017C00192 registered 03/07/2017

(iii) preventing the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country; or

(iv) determining whether the control order, or any succeeding control 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) the protection of the public from a terrorist act; or

(ii) preventing the provision of support for, or the facilitation of, a terrorist act; or

(iii) preventing the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country; or

(iv) determining whether the control order, or any succeeding control 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) the protection of the public from a terrorist act; or

(ii) preventing the provision of support for, or the facilitation of, a terrorist act; or

(iii) preventing the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country; or

(iv) determining whether the control order, or any succeeding control order, has been, or is being, complied with; and

(e) how much the use of such methods would be likely to prejudice:

(i) the protection of the public from a terrorist act; or

(ii) preventing the provision of support for, or the facilitation of, a terrorist act; or

Authorised Version C2017C00192 registered 03/07/2017

(iii) preventing the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country; or

(iv) determining whether the control order, or any succeeding control 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) 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; or

(vi) has contravened, is contravening, or will contravene, the control order; or

(vii) will contravene a succeeding control 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.

Authorised Version C2017C00192 registered 03/07/2017

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 control order warrant agency may apply for a warrant under section 46 in the circumstances mentioned in subsection 46(4).

Authorised Version C2017C00192 registered 03/07/2017

(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

Authorised Version C2017C00192 registered 03/07/2017

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.

Authorised Version C2017C00192 registered 03/07/2017

(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.

(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.

(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.

(8) A control order warrant must:

(a) state that the warrant is issued on the basis of a control order made in relation to a person; and

(b) specify the name of the person; and

(c) specify the date the control order was made; and

(d) state whether the control order is an interim control order or a confirmed control order.

Authorised Version C2017C00192 registered 03/07/2017

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

(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.

Authorised Version C2017C00192 registered 03/07/2017

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.

Authorised Version C2017C00192 registered 03/07/2017

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;

(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

Authorised Version C2017C00192 registered 03/07/2017

(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.

Authorised Version C2017C00192 registered 03/07/2017

(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 control order warrant issued on the ground that a control order was in force, that ground is taken to have ceased to exist if, and only if, neither that control order, nor any succeeding control 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.

(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.

Authorised Version C2017C00192 registered 03/07/2017

(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 control order warrants

(1) Within 6 months after a control order 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 a control order warrant under subsection 49(2);

(b) paragraph 57(1)(b), to the extent it applies to a control order warrant;

(c) subsection 63(1), to the extent it applies to lawfully intercepted information obtained under a control order warrant;

(d) subsection 63(2), to the extent it applies to interception warrant information that relates to a control order warrant;

(e) section 79, to the extent it applies to a restricted record obtained under a control order warrant;

Authorised Version C2017C00192 registered 03/07/2017

(f) section 79AA;
(g) subsection 103B(4).

(3) A failure to comply with subsection (1) or (2) does not affect the validity of a control order 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;
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.

Authorised Version C2017C00192 registered 03/07/2017

(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

Authorised Version C2017C00192 registered 03/07/2017

(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;

(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:

Authorised Version C2017C00192 registered 03/07/2017

(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

Authorised Version C2017C00192 registered 03/07/2017

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.

Authorised Version C2017C00192 registered 03/07/2017

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.

Authorised Version C2017C00192 registered 03/07/2017

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.

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:

(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.

Authorised Version C2017C00192 registered 03/07/2017

(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 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.

Authorised Version C2017C00192 registered 03/07/2017

(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.

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

Authorised Version C2017C00192 registered 03/07/2017

(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:

Authorised Version C2017C00192 registered 03/07/2017

(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;

(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.

Authorised Version C2017C00192 registered 03/07/2017

(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 Communicating 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;

(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 communicate that information to such persons, and in such manner, as are approved in writing by the Attorney-General.

(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.

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.

Authorised Version C2017C00192 registered 03/07/2017

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
  (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) the protection of the public from a terrorist act;
    (ii) preventing the provision of support for, or the facilitation of, a terrorist act;
    (iii) preventing the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country;
    (iv) determining whether a control 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 of the *Criminal Code* (Control orders);
    (vi) a preventative detention order law.

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.

Authorised Version C2017C00192 registered 03/07/2017

(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 purpose in relation to 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;
  (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;

Authorised Version C2017C00192 registered 03/07/2017

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 control order warrant—any of the following:

(i) the protection of the public from a terrorist act;

(ii) preventing the provision of support for, or the facilitation of, a terrorist act;

(iii) preventing the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country;

(iv) determining whether the control 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 of the *Criminal Code*;

(vi) a preventative detention order law.

(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.

Authorised Version C2017C00192 registered 03/07/2017

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 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

(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;

Authorised Version C2017C00192 registered 03/07/2017

and the originating agency is not the Australian Federal Police—to the Commissioner of Police; and

(ca) if:

(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

(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

Authorised Version C2017C00192 registered 03/07/2017

(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 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

(ja) if the information relates, or appears to relate, to a matter that may give rise to an investigation by the Independent

Authorised Version C2017C00192 registered 03/07/2017

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 for the purpose of providing the information to that foreign country; 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

Authorised Version C2017C00192 registered 03/07/2017

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.

68A Communicating information obtained by Secretary

(1) The Secretary of the Department may, personally, or by a person authorised by him or her, communicate to another person (including a foreign country) lawfully intercepted information or interception warrant information if:

(a) the information was communicated to the Secretary under paragraph 68(l) for the purpose of providing the information to a foreign country; and

(b) the communication of the information is for purposes connected with providing the information to the foreign country.

(2) A person to whom lawfully intercepted information or interception warrant information has been communicated under subsection (1) or this subsection may communicate that information to another person (including a foreign country) for purposes connected with providing the information to the foreign country.

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.

Authorised Version C2017C00192 registered 03/07/2017

(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;

Authorised Version C2017C00192 registered 03/07/2017

has been committed, the succeeding provisions of this section have effect, whether or not the interception contravened subsection 7(1).

(2) The person may communicate the relevant information to:
  (a) the Attorney-General;
  (b) the Director of Public Prosecutions;
  (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

Authorised Version C2017C00192 registered 03/07/2017

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) 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 warrant under section 11A, 11B or 11C), a person may give information obtained by the interception in evidence in an exempt

Authorised Version C2017C00192 registered 03/07/2017

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

Authorised Version C2017C00192 registered 03/07/2017

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, 74, 75, 75A, 76 or 76A permits a person to give in evidence in that proceeding information so obtained; and

Authorised Version C2017C00192 registered 03/07/2017

(b) for the purpose of determining the extent (if any) to which section 63A, 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.

Authorised Version C2017C00192 registered 03/07/2017

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 control 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 control 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 control order, or any succeeding control order, has been, or is being, complied with; and

(d) the interception occurred when the control order had been made, but had not come into force because it had not been served on the person to whom it relates; and

Authorised Version C2017C00192 registered 03/07/2017

(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:

(i) the protection of the public from a terrorist act; or

(ii) preventing the provision of support for, or the facilitation of, a terrorist act; or

(iii) preventing the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country;

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:

Authorised Version C2017C00192 registered 03/07/2017

(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.

Authorised Version C2017C00192 registered 03/07/2017

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:

Authorised Version C2017C00192 registered 03/07/2017

(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

Authorised Version C2017C00192 registered 03/07/2017

(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);

Authorised Version C2017C00192 registered 03/07/2017

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:

Authorised Version C2017C00192 registered 03/07/2017

(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 control order warrant—the name of the person to whom the relevant control order 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:

Authorised Version C2017C00192 registered 03/07/2017

(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 control order warrant—the name of the person to whom the relevant control order 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

Authorised Version C2017C00192 registered 03/07/2017

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.

Authorised Version C2017C00192 registered 03/07/2017

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.

Authorised Version C2017C00192 registered 03/07/2017

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 control order 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.

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,

Authorised Version C2017C00192 registered 03/07/2017

about the results of the inspections under subsections 83(1) and (3), 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 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.

Authorised Version C2017C00192 registered 03/07/2017

85A Annual report may cover notified breaches in relation to control order 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 control order 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,

Authorised Version C2017C00192 registered 03/07/2017

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;

(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

Authorised Version C2017C00192 registered 03/07/2017

(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

Authorised Version C2017C00192 registered 03/07/2017

(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 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,

Authorised Version C2017C00192 registered 03/07/2017

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.

Authorised Version C2017C00192 registered 03/07/2017

(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;

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

Authorised Version C2017C00192 registered 03/07/2017

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.

Authorised Version C2017C00192 registered 03/07/2017

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:

Authorised Version C2017C00192 registered 03/07/2017

(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;

Authorised Version C2017C00192 registered 03/07/2017

(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);

Authorised Version C2017C00192 registered 03/07/2017

(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

Authorised Version C2017C00192 registered 03/07/2017

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.

Authorised Version C2017C00192 registered 03/07/2017

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:

Authorised Version C2017C00192 registered 03/07/2017

(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

Authorised Version C2017C00192 registered 03/07/2017

(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

Authorised Version C2017C00192 registered 03/07/2017

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

Authorised Version C2017C00192 registered 03/07/2017

(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.

Authorised Version C2017C00192 registered 03/07/2017

(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

Authorised Version C2017C00192 registered 03/07/2017

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:

Authorised Version C2017C00192 registered 03/07/2017

(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.

Authorised Version C2017C00192 registered 03/07/2017

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 mutual assistance requests

The report must set out the number of occasions on which lawfully intercepted information or interception warrant information was provided to a foreign country under paragraph 68(l) or section 68A in connection with an authorisation under subsection 13A(1) of the *Mutual Assistance in Criminal Matters Act 1987*.

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

Authorised Version C2017C00192 registered 03/07/2017

(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

(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

Authorised Version C2017C00192 registered 03/07/2017

(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

Authorised Version C2017C00192 registered 03/07/2017

(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 control order 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 control order 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 control order information; and
(b) if the chief officer is satisfied that the information is not control order 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 control order 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:

control order information means information that, if made public, could reasonably be expected to enable a reasonable person to conclude that:

Authorised Version C2017C00192 registered 03/07/2017

(a) a control order 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 control order warrant is likely to be, or is not likely to be, in force in relation to a particular person.

Ministerial report means a report the Minister prepares under this Division.

Authorised Version C2017C00192 registered 03/07/2017

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.

Authorised Version C2017C00192 registered 03/07/2017

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.

Authorised Version C2017C00192 registered 03/07/2017

(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*).

Authorised Version C2017C00192 registered 03/07/2017

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

Authorised Version C2017C00192 registered 03/07/2017

(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.

Authorised Version C2017C00192 registered 03/07/2017

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.

Authorised Version C2017C00192 registered 03/07/2017

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.

Authorised Version C2017C00192 registered 03/07/2017

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.

Authorised Version C2017C00192 registered 03/07/2017

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).

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

Authorised Version C2017C00192 registered 03/07/2017

(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 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.

Authorised Version C2017C00192 registered 03/07/2017

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

Authorised Version C2017C00192 registered 03/07/2017

(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

Authorised Version C2017C00192 registered 03/07/2017

(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.

Authorised Version C2017C00192 registered 03/07/2017

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.

Authorised Version C2017C00192 registered 03/07/2017

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.

Authorised Version C2017C00192 registered 03/07/2017

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) If, under paragraph 15B(d) of the *Mutual Assistance in Criminal Matters Act 1987*, a foreign country intends to request the Attorney-General to arrange for access to 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, or investigative proceeding, relating to a criminal matter involving a serious foreign contravention;

then the foreign country may request the Australian Federal Police to arrange for the preservation of those stored communications.

(2) The request to the Australian Federal Police must:

Authorised Version C2017C00192 registered 03/07/2017

(a) be in writing; and
(b) specify the name of the authority concerned with the criminal matter; and
(c) specify the serious foreign contravention that is the subject of the investigation or investigative 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 foreign country 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 foreign country 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 foreign country intends to make a request under paragraph 15B(d) of the *Mutual Assistance in Criminal Matters Act 1987* to access 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:
(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 after the Attorney-General has given an authorisation in relation to the warrant under section 15B of the *Mutual Assistance in Criminal Matters Act 1987*—when the warrant ceases to be in force.

Authorised Version C2017C00192 registered 03/07/2017

107R Revoking a foreign preservation notice

(1) If:

(a) a foreign country makes a request under section 107P to preserve 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 foreign country did not make a request to the Attorney-General under paragraph 15B(d) of the *Mutual Assistance in Criminal Matters Act 1987* 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) a foreign country makes a request under section 107P to preserve 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 foreign country makes a request to the Attorney-General under paragraph 15B(d) of the *Mutual Assistance in Criminal Matters Act 1987* to arrange for access to those communications; and

(d) the Attorney-General refuses that 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:

Authorised Version C2017C00192 registered 03/07/2017

(a) a foreign country makes a request under section 107P to preserve 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 foreign country 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.

Authorised Version C2017C00192 registered 03/07/2017

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.

Authorised Version C2017C00192 registered 03/07/2017

(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.

Authorised Version C2017C00192 registered 03/07/2017

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

Authorised Version C2017C00192 registered 03/07/2017

(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

(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:

(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

Authorised Version C2017C00192 registered 03/07/2017

(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.

Authorised Version C2017C00192 registered 03/07/2017

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.

Authorised Version C2017C00192 registered 03/07/2017

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;

Authorised Version C2017C00192 registered 03/07/2017

(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:

Authorised Version C2017C00192 registered 03/07/2017

(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.

Authorised Version C2017C00192 registered 03/07/2017

(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

Authorised Version C2017C00192 registered 03/07/2017

(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:

Authorised Version C2017C00192 registered 03/07/2017

(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.

Authorised Version C2017C00192 registered 03/07/2017

(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.

Authorised Version C2017C00192 registered 03/07/2017

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) in the case of an application other than a mutual assistance application—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) in the case of a mutual assistance application—the investigation or investigative proceeding, by the foreign country 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

Authorised Version C2017C00192 registered 03/07/2017

(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) In the case of an application other than a mutual 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) In the case of a mutual assistance application, the matters to which the issuing authority must have regard are:

Authorised Version C2017C00192 registered 03/07/2017

(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, to the extent that this is possible to determine from information obtained from the foreign country 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.

Authorised Version C2017C00192 registered 03/07/2017

(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.

Authorised Version C2017C00192 registered 03/07/2017

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:

Authorised Version C2017C00192 registered 03/07/2017

(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.

Authorised Version C2017C00192 registered 03/07/2017

(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:

Authorised Version C2017C00192 registered 03/07/2017

(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.

Authorised Version C2017C00192 registered 03/07/2017

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).

Authorised Version C2017C00192 registered 03/07/2017

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

Authorised Version C2017C00192 registered 03/07/2017

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.

Authorised Version C2017C00192 registered 03/07/2017

(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*).

Authorised Version C2017C00192 registered 03/07/2017

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.

Authorised Version C2017C00192 registered 03/07/2017

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.

Authorised Version C2017C00192 registered 03/07/2017

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

Authorised Version C2017C00192 registered 03/07/2017

(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.

Authorised Version C2017C00192 registered 03/07/2017

(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 Communicating 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 communicate that information to such persons, and in such manner, as are approved in writing by the Attorney-General.

Authorised Version C2017C00192 registered 03/07/2017

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), 139B(2) or 139C(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;

(aa) preservation notice information;

(b) stored communications warrant information.

Authorised Version C2017C00192 registered 03/07/2017

(2) In the case of information obtained by the agency other than through the execution of a warrant issued as a result of a mutual 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 subsection 13A(1) of the *Mutual Assistance in Criminal Matters Act 1987* in respect of the information.

(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.

Authorised Version C2017C00192 registered 03/07/2017

(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 a mutual assistance application, the purposes are purposes connected with:
  (a) providing the information to the foreign country, or an appropriate authority of the foreign country, to which the application relates; or
  (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

Authorised Version C2017C00192 registered 03/07/2017

(4A), 139B(2) or 139C(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 control orders and preventative detention 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), 139A(2) or 139C(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:

(a) 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 of the *Criminal Code* (Control orders); or

(b) a preventative detention order law.

139C Dealing for purposes relating to continuing detention orders

(1) An officer or staff member of:

(a) the Australian Federal Police; or

(b) the Police Force of a State;

Authorised Version C2017C00192 registered 03/07/2017

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), 139A(2) or 139B(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, Division 105A of the *Criminal Code* (continuing detention orders).

140 Dealing with information if access suspected to be unlawful

(1) A person may communicate information to the Attorney-General, 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

Authorised Version C2017C00192 registered 03/07/2017

(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;

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, 139B or 139C, 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 a mutual assistance application to foreign country

(1) Despite subsection 139(4A) and section 142, a person may only communicate information, obtained through the execution of a warrant issued as a result of a mutual assistance application, to the foreign country to which the application relates, subject to the following conditions:

Authorised Version C2017C00192 registered 03/07/2017

(a) that the information will only be used for the purposes for which the foreign country 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) A determination made 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

Authorised Version C2017C00192 registered 03/07/2017

(ii) the irregularity is not a substantial defect or irregularity; and

(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.

Authorised Version C2017C00192 registered 03/07/2017

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

Authorised Version C2017C00192 registered 03/07/2017

(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.

Authorised Version C2017C00192 registered 03/07/2017

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), 139B(2) or 139C(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.

Authorised Version C2017C00192 registered 03/07/2017

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);

Authorised Version C2017C00192 registered 03/07/2017

(g) each request for mutual assistance, being a request to which a mutual 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.

Authorised Version C2017C00192 registered 03/07/2017

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).

Authorised Version C2017C00192 registered 03/07/2017

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.

Authorised Version C2017C00192 registered 03/07/2017

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

Authorised Version C2017C00192 registered 03/07/2017

(b) the relevant statistics about telephone applications for stored communications warrants that the agency made during that year; and

(c) the relevant statistics about mutual assistance applications that the agency made during that year; and

(d) for each offence (the ***foreign offence***) against a law of a foreign country in respect of which a stored communications warrant was issued as a result of a mutual assistance application made by the agency during the year—the offence (if any), under a law of the Commonwealth, or of a State or a Territory, that is of the same nature as, or a substantially similar nature to, the foreign 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 mutual 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 offence (the ***foreign offence***) against a law of a foreign country in respect of which a stored communications warrant was issued as a result of a mutual assistance application made during the year—the offence (if any), under a law of the Commonwealth, or of a State or a Territory, that is of the same nature as, or a substantially similar nature to, the foreign offence.

Authorised Version C2017C00192 registered 03/07/2017

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 mutual assistance requests

The report must set out the number of occasions on which lawfully accessed information or stored communications warrant information was provided to a foreign country under subsection 139(1) or section 142 in connection with an authorisation under subsection 13A(1) of the *Mutual Assistance in Criminal Matters Act 1987*.

Authorised Version C2017C00192 registered 03/07/2017

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.

Authorised Version C2017C00192 registered 03/07/2017

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;

Authorised Version C2017C00192 registered 03/07/2017

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.

Authorised Version C2017C00192 registered 03/07/2017

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.

Authorised Version C2017C00192 registered 03/07/2017

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.

Authorised Version C2017C00192 registered 03/07/2017

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.

Authorised Version C2017C00192 registered 03/07/2017

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.

Authorised Version C2017C00192 registered 03/07/2017

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*.

Authorised Version C2017C00192 registered 03/07/2017

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.

Authorised Version C2017C00192 registered 03/07/2017

(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.

Authorised Version C2017C00192 registered 03/07/2017

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 Minister 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.

Authorised Version C2017C00192 registered 03/07/2017

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

Authorised Version C2017C00192 registered 03/07/2017

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.

Authorised Version C2017C00192 registered 03/07/2017

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.

Authorised Version C2017C00192 registered 03/07/2017

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.

Authorised Version C2017C00192 registered 03/07/2017

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.

Authorised Version C2017C00192 registered 03/07/2017

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

Authorised Version C2017C00192 registered 03/07/2017

(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.

Authorised Version C2017C00192 registered 03/07/2017

Division 4A—Foreign law enforcement

Subdivision A—Primary disclosures

180A Authorisations for access to existing information or documents—enforcement of the criminal law of a foreign country

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 the enforcement of the criminal law of a foreign country.

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.

(5) The authorised officer must not make the authorisation unless he or she is satisfied that:

Authorised Version C2017C00192 registered 03/07/2017

(a) the disclosure is reasonably necessary for the enforcement of the criminal law of a foreign country; and
(b) the disclosure is appropriate in all the circumstances.

180B Authorisations for access to prospective information or documents—enforcement of the criminal law of a foreign country

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 the *Mutual Assistance in Criminal Matters Act 1987*; and
(b) the authorised officer is satisfied that the disclosure is reasonably necessary for the investigation of an offence against the law of a foreign country that:
(i) is punishable by imprisonment for 3 years or more, imprisonment for life or the death penalty; or
(ii) involves an act or omission that, if it had occurred in Australia, would have constituted a serious offence within the meaning of section 5D of the *Telecommunications (Interception and Access) Act 1979*; and
(c) the authorised officer is satisfied that the disclosure is appropriate in all the circumstances.

Authorised Version C2017C00192 registered 03/07/2017

(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 Australian Federal Police, if the authorised officer is satisfied that the extension is:

(a) reasonably necessary for the investigation of an offence against the law of a foreign country that:

(i) is punishable by imprisonment for 3 years or more, imprisonment for life or the death penalty; or

(ii) involves an act or omission that, if it had occurred in Australia, would have constituted a serious offence within the meaning of section 5D of the *Telecommunications (Interception and Access) Act 1979*; 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.

Authorised Version C2017C00192 registered 03/07/2017

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 the investigation of an offence against the law of a foreign country that:

(i) is punishable by imprisonment for 3 years or more, imprisonment for life or the death penalty; or

(ii) involves an act or omission that, if it had occurred in Australia, would have constituted a serious offence within the meaning of section 5D of the *Telecommunications (Interception and Access) Act 1979*; 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—enforcement of the criminal law of a foreign country

(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:

(a) the disclosure is reasonably necessary for the enforcement of the criminal law of a foreign country; and

Authorised Version C2017C00192 registered 03/07/2017

(b) the disclosure is appropriate in all the circumstances.

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* (continuing detention 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:

(i) for the enforcement of the criminal law; or

(ia) for the purposes of Division 105A of the *Criminal Code* (continuing detention orders); or

(ii) for the enforcement of a law imposing a pecuniary penalty; or

(iii) for the protection of the public revenue; and

Authorised Version C2017C00192 registered 03/07/2017

(d) in any case—the disclosure or use is appropriate in all the circumstances.

Subdivision C—Conditions of disclosure to foreign country

180E Disclosing information etc. obtained to foreign country

(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 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 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.

Authorised Version C2017C00192 registered 03/07/2017

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.

Authorised Version C2017C00192 registered 03/07/2017

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

Authorised Version C2017C00192 registered 03/07/2017

(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 Minister 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.

Authorised Version C2017C00192 registered 03/07/2017

180K Further information

(1) The Minister may require the Director-General of Security to give to the Minister, 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 Minister 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 Minister 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 Minister must not issue a journalist information warrant unless the Minister 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

Authorised Version C2017C00192 registered 03/07/2017

(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 Minister 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 Minister 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 Minister 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 Minister; and

(e) either:

(i) the issuing of the warrant is authorised under subsection (3); or

Authorised Version C2017C00192 registered 03/07/2017

(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 Minister; or
(b) if the Director-General is satisfied that the Minister is not readily available or contactable—any of the following Ministers:
(i) the Prime Minister;
(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 Minister may revoke the warrant at any time before the end of the specified period.

Authorised Version C2017C00192 registered 03/07/2017

Copies of warrant and other documents

(8) Immediately after issuing a journalist information warrant under this section, the Director-General must give the Minister:
  (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 Minister may revoke the warrant at any time before the end of the specified period.

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

Authorised Version C2017C00192 registered 03/07/2017

is satisfied that the grounds on which the warrant was issued have ceased to exist, he or she must:

(a) forthwith inform the Minister 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.

Authorised Version C2017C00192 registered 03/07/2017

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
  (b) refuse to issue a journalist information warrant.

Authorised Version C2017C00192 registered 03/07/2017

(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

Authorised Version C2017C00192 registered 03/07/2017

(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:

Authorised Version C2017C00192 registered 03/07/2017

(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 Minister 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.

Authorised Version C2017C00192 registered 03/07/2017

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.

Authorised Version C2017C00192 registered 03/07/2017

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

Authorised Version C2017C00192 registered 03/07/2017

(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.

Authorised Version C2017C00192 registered 03/07/2017

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.

Authorised Version C2017C00192 registered 03/07/2017

(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* (continuing detention 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;

Authorised Version C2017C00192 registered 03/07/2017

(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* (continuing detention 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.

Authorised Version C2017C00192 registered 03/07/2017

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* (continuing detention 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:

Authorised Version C2017C00192 registered 03/07/2017

(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

(iia) for the purposes of Division 105A of the *Criminal Code* (continuing detention 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.

Authorised Version C2017C00192 registered 03/07/2017

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.

Authorised Version C2017C00192 registered 03/07/2017

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* (continuing detention 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*).

Authorised Version C2017C00192 registered 03/07/2017

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.

Authorised Version C2017C00192 registered 03/07/2017

(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

Authorised Version C2017C00192 registered 03/07/2017

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*.

Authorised Version C2017C00192 registered 03/07/2017

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

Authorised Version C2017C00192 registered 03/07/2017

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 Minister 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

Authorised Version C2017C00192 registered 03/07/2017

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

Authorised Version C2017C00192 registered 03/07/2017

(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

Authorised Version C2017C00192 registered 03/07/2017

(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:

Authorised Version C2017C00192 registered 03/07/2017

(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

Authorised Version C2017C00192 registered 03/07/2017

(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).

Authorised Version C2017C00192 registered 03/07/2017

(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);

Authorised Version C2017C00192 registered 03/07/2017

(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

Authorised Version C2017C00192 registered 03/07/2017

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;

Authorised Version C2017C00192 registered 03/07/2017

whichever happens earlier.

(4) Subsection (3) does not affect the operation of section 185.

Authorised Version C2017C00192 registered 03/07/2017

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.

(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

(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

Authorised Version C2017C00192 registered 03/07/2017

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.

Authorised Version C2017C00192 registered 03/07/2017

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

(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*.

Authorised Version C2017C00192 registered 03/07/2017

(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

Authorised Version C2017C00192 registered 03/07/2017

(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.

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.

Authorised Version C2017C00192 registered 03/07/2017

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:

Authorised Version C2017C00192 registered 03/07/2017

(a) endanger a person's safety; or
(b) prejudice an investigation or prosecution; or
(c) compromise any enforcement agency's operational activities or methodologies.

Authorised Version C2017C00192 registered 03/07/2017

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.

Authorised Version C2017C00192 registered 03/07/2017

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 Schedule 5 to the *Broadcasting Services Act 1992*); 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;

Authorised Version C2017C00192 registered 03/07/2017

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.

Authorised Version C2017C00192 registered 03/07/2017

(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.

Authorised Version C2017C00192 registered 03/07/2017

(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	The following: (a) any information that is one or both of the following: (i) any name or address information; (ii) any other information for identification purposes; relating to the relevant service, being information used by the service provider for the purposes of identifying the subscriber of the relevant service; (b) any information relating to any contract, agreement or arrangement relating to the relevant service, or to any related account, service or device; (c) any information that is one or both of the following: (i) billing or payment information; (ii) contact information; relating to the relevant service, being information used by the service provider in relation to the relevant service; (d) any identifiers relating to the relevant service or any related account, service or device, being information used by the service provider in

Authorised Version C2017C00192 registered 03/07/2017

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.

Authorised Version C2017C00192 registered 03/07/2017

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.

Authorised Version C2017C00192 registered 03/07/2017

(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.

Authorised Version C2017C00192 registered 03/07/2017

(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.

Authorised Version C2017C00192 registered 03/07/2017

(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.

Authorised Version C2017C00192 registered 03/07/2017

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.

Authorised Version C2017C00192 registered 03/07/2017

(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;

Authorised Version C2017C00192 registered 03/07/2017

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.

Authorised Version C2017C00192 registered 03/07/2017

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

Authorised Version C2017C00192 registered 03/07/2017

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

Authorised Version C2017C00192 registered 03/07/2017

(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).

Authorised Version C2017C00192 registered 03/07/2017

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:

Authorised Version C2017C00192 registered 03/07/2017

(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.

Authorised Version C2017C00192 registered 03/07/2017

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.

Authorised Version C2017C00192 registered 03/07/2017

(5) The ACMA may take into account any other matter it considers relevant.

Authorised Version C2017C00192 registered 03/07/2017

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.

Authorised Version C2017C00192 registered 03/07/2017

(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 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

Authorised Version C2017C00192 registered 03/07/2017

(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:

Authorised Version C2017C00192 registered 03/07/2017

(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.

Authorised Version C2017C00192 registered 03/07/2017

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).

Authorised Version C2017C00192 registered 03/07/2017

(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:

Authorised Version C2017C00192 registered 03/07/2017

(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).

Authorised Version C2017C00192 registered 03/07/2017

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.

Authorised Version C2017C00192 registered 03/07/2017

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:

Authorised Version C2017C00192 registered 03/07/2017

(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.

Authorised Version C2017C00192 registered 03/07/2017

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

Authorised Version C2017C00192 registered 03/07/2017

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.

Authorised Version C2017C00192 registered 03/07/2017

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.

Authorised Version C2017C00192 registered 03/07/2017

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

Authorised Version C2017C00192 registered 03/07/2017

(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.

Authorised Version C2017C00192 registered 03/07/2017

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.

Authorised Version C2017C00192 registered 03/07/2017

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:

Authorised Version C2017C00192 registered 03/07/2017

(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

Authorised Version C2017C00192 registered 03/07/2017

(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.

Authorised Version C2017C00192 registered 03/07/2017

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*; 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*.

(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;

(b) the carrier or carriage service provider changing the location of notifiable equipment (including moving equipment outside Australia);

Authorised Version C2017C00192 registered 03/07/2017

(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

Authorised Version C2017C00192 registered 03/07/2017

(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.

Authorised Version C2017C00192 registered 03/07/2017

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.

Authorised Version C2017C00192 registered 03/07/2017

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.

Authorised Version C2017C00192 registered 03/07/2017

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.

Authorised Version C2017C00192 registered 03/07/2017

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.

Authorised Version C2017C00192 registered 03/07/2017

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.

Authorised Version C2017C00192 registered 03/07/2017

(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.

Authorised Version C2017C00192 registered 03/07/2017

(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.

Authorised Version C2017C00192 registered 03/07/2017

(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.

Authorised Version C2017C00192 registered 03/07/2017

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

Authorised Version C2017C00192 registered 03/07/2017

(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*.

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

Authorised Version C2017C00192 registered 03/07/2017

(b) necessary or convenient to be prescribed for carrying out or giving effect to this Act.

Authorised Version C2017C00192 registered 03/07/2017

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

Authorised Version C2017C00192 registered 03/07/2017

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.

Authorised Version C2017C00192 registered 03/07/2017

Endnote 2—Abbreviation key

ad = added or inserted

am = amended

amdt = amendment

c = clause(s)

C[x] = Compilation No. x

Ch = Chapter(s)

def = definition(s)

Dict = Dictionary

disallowed = disallowed by Parliament

Div = Division(s)

ed = editorial change

exp = expires/expired or ceases/ceased to have effect

F = Federal Register of Legislation

gaz = gazette

LA = *Legislation Act 2003*

LIA = *Legislative Instruments Act 2003*

(md) = misdescribed amendment can be given effect

(md not incorp) = misdescribed amendment cannot be given effect

mod = modified/modification

No. = Number(s)

o = order(s)

Ord = Ordinance

orig = original

par = paragraph(s)/subparagraph(s) /sub-subparagraph(s)

pres = present

prev = previous

(prev…) = previously

Pt = Part(s)

r = regulation(s)/rule(s)

reloc = relocated

renum = renumbered

rep = repealed

rs = repealed and substituted

s = section(s)/subsection(s)

Sch = Schedule(s)

Sdiv = Subdivision(s)

SLI = Select Legislative Instrument

SR = Statutory Rules

Sub-Ch = Sub-Chapter(s)

SubPt = Subpart(s)

underlining = whole or part not commenced or to be commenced

Authorised Version C2017C00192 registered 03/07/2017

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 (*see Gazette* 1980, No. G21, p. 2)	
Telecommunications (Interception) Amendment Act 1979	181, 1979	4 Dec 1979	1 June 1980 (*see* s. 2 and *Gazette* 1980, No. G21, p. 2)	—
Director of Public Prosecutions (Consequential Amendments) Act 1983	114, 1983	14 Dec 1983	s. 8(1): 16 Dec 1985 (*see* s. 2(2)) s. 8(2): 16 Dec 1985 (*see* s. 2(3)) Remainder: 5 Mar 1984 (*see* s. 2(1) and *Gazette* 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

Authorised Version C2017C00192 registered 03/07/2017

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	1 Feb 1987 (*see* s. 2 and *Gazette* 1987, No. S13)	—
as amended by				
Crimes Legislation Amendment Act 1991	28, 1991	4 Mar 1991	s. 74(3): *(a)*	—
Telecommunications (Interception) Amendment Act 1987	89, 1987	5 June 1987	ss. 1 and 2: Royal Assent Remainder: 1 Sept 1988 (*see Gazette* 1988, No. S256) ss. 5(1)(a), (2), 6 and 8: 16 Dec 1987 (*see* 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	Part X (ss. 53, 54): Royal Assent *(b)*	—
Crimes Legislation Amendment Act 1987	120, 1987	16 Dec 1987	ss. 55 and 59: Royal Assent *(c)* ss. 56–58: *(c)* ss. 60–67: *(c)*	—
Extradition (Repeal and Consequential Provisions) Act 1988	5, 1988	9 Mar 1988	s. 5: 1 Dec 1988 (*see Gazette* 1988, No. S366) *(d)*	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 *Gazette* 1988, No. S256) Remainder: Royal Assent	—
Crimes Legislation Amendment Act (No. 2) 1988	66, 1988	15 June 1988	Part VI (ss. 25–28): *(e)*	—

Authorised Version C2017C00192 registered 03/07/2017

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 Gazette* 1988, No. S402) ss. 14, 23(3) and 26(2): 30 June 1989 (*see Gazette* 1989, No. S216) Remainder: Royal Assent	—
Telecommunications and Postal Services (Transitional Provisions and Consequential Amendments) Act 1989	63, 1989	19 June 1989	ss. 1 and 2: Royal Assent Part 5 (ss. 17, 18): 30 June 1989 (*see Gazette* 1989, No. S216) Remainder: 1 July 1989 (*see Gazette* 1989, No. S230)	—
as amended by				
Transport and Communications Legislation Amendment Act 1990	11, 1991	21 Jan 1991	s. 45: *(f)*	—
Law and Justice Legislation Amendment Act 1989	11, 1990	17 Jan 1990	ss. 50, 51(1)(a) and 52–56: 14 Feb 1990 *(g)* s. 51(1)(b) and (2): Royal Assent *(g)*	s 51(2)

Authorised Version C2017C00192 registered 03/07/2017

Endnote 3—Legislation history

Act	Number and year	Assent	Commencement	Application, saving and transitional provisions
Crimes Legislation Amendment Act 1991	28, 1991	4 Mar 1991	ss. 60, 61(1), 64–66 and 68–72: Royal Assent *(h)* ss. 61(2), 62, 63, 67 and 73: 29 Apr 1991 (*see Gazette* 1991, No. S108) *(h)*	s 73
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 *Gazette* 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 Gazette* 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: Royal Assent *(i)* s. 27: 18 Apr 1995 *(i)*	s. 14
International War Crimes Tribunals (Consequential Amendments) Act 1995	19, 1995	29 Mar 1995	s. 3: 28 Aug 1995 (*see Gazette* 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)

Authorised Version C2017C00192 registered 03/07/2017

Endnote 3—Legislation history

Act	Number and year	Assent	Commencement	Application, saving and transitional provisions
Statute Law Revision Act 1996	43, 1996	25 Oct 1996	Schedule 5 (items 147–149): Royal Assent *(j)*	—
Telecommunications (Transitional Provisions and Consequential Amendments) Act 1997	59, 1997	3 May 1997	Schedule 1 (items 51–55): 1 July 1997 *(k)*	—
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 (*see Gazette* 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	Schedule 2: 22 July 1999 (*see Gazette* 1999, No. S337) *(l)*	—
Public Employment (Consequential and Transitional) Amendment Act 1999	146, 1999	11 Nov 1999	Schedule 1 (item 918): 5 Dec 1999 (*see Gazette* 1999, No. S584) *(m)*	—
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	Schedule 3 (items 1, 62–81): *(n)*	—

Authorised Version C2017C00192 registered 03/07/2017

Endnote 3—Legislation history

Act	Number and year	Assent	Commencement	Application, saving and transitional provisions
Australian Federal Police Legislation Amendment Act 2000	9, 2000	7 Mar 2000	2 July 2000 (*see Gazette* 2000, No. S328)	Sch 3 (items 20, 32, 34, 35)
Telecommunications (Interception) Legislation Amendment Act 2000	63, 2000	22 June 2000	Schedule 3 (items 2, 3): *(o)* Remainder: Royal Assent	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 Schedule 47: *(p)*	s 4(1) and (2)
Corporations (Repeals, Consequentials and Transitionals) Act 2001	55, 2001	28 June 2001	ss. 4–14 and Schedule 3 (items 513–515): 15 July 2001 (*see Gazette* 2001, No. S285) *(q)*	s 4–14
National Crime Authority Legislation Amendment Act 2001	135, 2001	1 Oct 2001	Schedules 1–7 and 9–12: 12 Oct 2001 (*see Gazette* 2001, No. S428) Schedule 8: 13 Oct 2001 (*see Gazette* 2001, No. S428) Remainder: Royal Assent	—
Cybercrime Act 2001	161, 2001	1 Oct 2001	21 Dec 2001 (*see Gazette* 2001, No. S529)	—

Authorised Version C2017C00192 registered 03/07/2017

Act	Number and year	Assent	Commencement	Application, saving and transitional provisions
as amended by				
Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Act (No. 2) 2004	127, 2004	31 Aug 2004	(*see* 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 (*see* s. 2(1) and *Gazette* 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 (*see* s. 2(1) and *Gazette* 2002, No. GN44)	—
Australian Crime Commission Establishment Act 2002	125, 2002	10 Dec 2002	Schedule 2 (items 190–224): 1 Jan 2003 Schedule 3 (item 17): *(r)*	—
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)

Authorised Version C2017C00192 registered 03/07/2017

Endnote 3—Legislation history

Act	Number and year	Assent	Commencement	Application, saving and transitional provisions
Telecommunications Interception and Other Legislation Amendment Act 2003	113, 2003	12 Nov 2003	Schedule 1: 6 Feb 2004 (*see Gazette* 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	Schedule 1 (items 25–29, 31): 1 Mar 2005 Schedule 5 (item 9): *(s)*	Sch 1 (item 31)
as amended by				
Telecommunications (Interception) Amendment Act 2006	40, 2006	3 May 2006	Schedule 1 (item 16): (*see* 40, 2006 below)	—
Telecommunications (Interception) Amendment (Stored Communications) Act 2004	148, 2004	14 Dec 2004	15 Dec 2004	—
Crimes Legislation Amendment (Telecommunications Interception and Other Measures) Act 2005	95, 2005	6 July 2005	Schedule 1: 1 Mar 2005 Schedule 2 (items 1, 2, 9): 17 Dec 2005 (*see* F2005L04095) Schedule 2 (item 4): *(t)* Schedule 2 (item 5): *(t)* Schedule 2 (item 15): 1 June 1980 Remainder: Royal Assent	—

Authorised Version C2017C00192 registered 03/07/2017

Act	Number and year	Assent	Commencement	Application, saving and transitional provisions
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	Schedules 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 (*see* F2006L03104) Remainder: Royal Assent	—
Telecommunications (Interception) Amendment Act 2006	40, 2006	3 May 2006	Schedules 1–3: 13 June 2006 (*see* F2006L01623) Schedule 4: 1 July 2006 Schedule 5: 3 Nov 2006 Schedule 6 (items 1, 3): *(u)* Schedule 6 (item 8): *(u)* Remainder: Royal Assent	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)	—

Authorised Version C2017C00192 registered 03/07/2017

Endnote 3—Legislation history

Act	Number and year	Assent	Commencement	Application, saving and transitional provisions
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)	—
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	—

Authorised Version C2017C00192 registered 03/07/2017

Endnote 3—Legislation history

Act	Number and year	Assent	Commencement	Application, saving and transitional provisions
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) 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	—

Authorised Version C2017C00192 registered 03/07/2017

Endnote 3—Legislation history

Act	Number and year	Assent	Commencement	Application, saving and transitional provisions
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	—
Corporations Amendment (No. 1) Act 2010	131, 2010	24 Nov 2010	Schedule 1 (item 21): 13 Dec 2010 (*see* 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	—

Authorised Version C2017C00192 registered 03/07/2017

Act	Number and year	Assent	Commencement	Application, saving and transitional provisions
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)
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

Authorised Version C2017C00192 registered 03/07/2017

Endnote 3—Legislation history

Act	Number and year	Assent	Commencement	Application, saving and transitional provisions
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)	—
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

Authorised Version C2017C00192 registered 03/07/2017

Act	Number and year	Assent	Commencement	Application, saving and transitional provisions
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)	—
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 (item 1), Sch 1 (items 29–36, 54, 55) and Sch 1 (items 56–58)

Authorised Version C2017C00192 registered 03/07/2017

Endnote 3—Legislation history

Act	Number and year	Assent	Commencement	Application, saving and transitional provisions
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)	—

(a) The *Intelligence and Security (Consequential Amendments) Act 1986* was amended by subsection 74(3) of the *Crimes Legislation Amendment Act 1991*, subsection 2(7) of which provides as follows:

(7) Subsection 74(3) and Part 3 of Schedule 2 are taken to have commenced immediately after the commencement of section 25 of the *Intelligence and Security (Consequential Amendments) Act 1986*.

Section 25 commenced on 1 February 1987 (*see Gazette* 1987, No. S13).

(b) The *Telecommunications (Interception) Amendment Act 1987* was amended by Part X (sections 53 and 54) only of the *Crimes Legislation Amendment Act 1987*, subsection 2(3) of which provides as follows:

(3) Sections 53, 54, 55 and 59 shall come into operation on the day on which this Act receives the Royal Assent.

(c) The *Telecommunications (Interception and Access) Act 1979* was amended by sections 55–67 only of the *Crimes Legislation Amendment Act 1987*, subsections 2(3)–(5) of which provide as follows:

(3) Sections 53, 54, 55 and 59 shall come into operation on the day on which this Act receives the Royal Assent.

(4) Sections 56, 57 and 58 shall come into operation immediately after the commencement of subsection 5(2) and section 8 of the *Telecommunications (Interception) Amendment Act 1987*.

(5) Sections 60 to 67, inclusive, shall come into operation immediately after the commencement of section 21 of the *Telecommunications (Interception) Amendment Act 1987*.

Authorised Version C2017C00192 registered 03/07/2017

Subsection 5(2) and section 8 commenced on 16 December 1987.

Section 21 commenced on 1 September 1988 (*see Gazette* 1988, No. S256).

(d) The *Telecommunications (Interception and Access) Act 1979* was amended by section 5 only of the *Extradition (Repeal and Consequential Provisions) Act 1988*, subsection 2(3)(a) of which provides as follows:

(3) This Act, in so far as it provides for the amendment of the *Telecommunications (Interception) Act 1979* as set out in the Schedule, shall come into operation:

(a) when the *Extradition Act 1988* comes into operation; or

(e) The *Telecommunications (Interception and Access) Act 1979* was amended by Part VI (sections 25–28) only of the *Crimes Legislation Amendment Act (No. 2) 1988*, subsection 2(5) of which provides as follows:

(5) Part VI of this Act commences, or shall be taken to have commenced, as the case requires, immediately after the commencement of section 21 of the *Telecommunications (Interception) Amendment Act 1987*.

Section 21 commenced on 1 September 1988 (*see Gazette* 1988, No. S256).

(f) The *Telecommunications and Postal Services (Transitional Provisions and Consequential Amendments) Act 1989* was amended by section 45 only of the *Transport and Communications Legislation Amendment Act 1990*, subsection 2(13)(e) of which provides as follows:

(13) The amendments made in the Schedule are taken to have commenced as follows:

(e) each amendment of a provision of, or an item in a Schedule to, the *Telecommunications and Postal Services (Transitional Provisions and Consequential Amendments) Act 1989* is taken to have commenced immediately after the commencement of the provision, or item, concerned.

The amendments made by section 45 commenced on 1 July 1989 (*see Gazette* 1989, No. S230).

(g) The *Telecommunications (Interception and Access) Act 1979* was amended by sections 50–56 only of the *Law and Justice Legislation Amendment Act 1989*, subsections 2(1) and (5)(b) of which provide as follows:

(1) Subject to this section, this Act commences on the 28th day after the day on which it receives the Royal Assent.

(5) Sections 12 and 13, paragraph 51(1)(b) and subsection 51(2) commence:

(b) on the day on which this Act receives the Royal Assent;

Authorised Version C2017C00192 registered 03/07/2017

(h) The *Telecommunications (Interception and Access) Act 1979* was amended by sections 60–73 only of the *Crimes Legislation Amendment Act 1991*, subsections 2(1) and (2) of which provide as follows:

(1) Subject to this section, this Act commences on the day on which it receives the Royal Assent.

(2) Section 23, paragraph 30(b), subsection 61(2) and sections 62, 63, 67 and 73 commence on a day to be fixed by Proclamation, being the day on which Schedule 1(3) to the *State Drug Crime Commission (Amendment) Act 1990* of New South Wales commences.

(i) The *Telecommunications (Interception and Access) Act 1979* was amended by sections 14 and 27 only of the *Evidence (Transitional Provisions and Consequential Amendments) Act 1995*, subsections 2(1) and (13) of which provide as follows:

(1) This Part and Parts 2 and 3 commence on the day on which this Act receives the Royal Assent.

(13) Section 27 of this Act and the Schedule to this Act commence:

(a) on the day on which sections 153 and 155 of the *Evidence Act 1995* commence; or

(b) if those sections commence on different days—the first day on which both of those sections are in force.

(j) The *Telecommunications (Interception and Access) Act 1979* was amended by Schedule 5 (items 147–149) only of the *Statute Law Revision Act 1996*, subsection 2(1) of which provides as follows:

(1) Subject to subsections (2) and (3), this Act commences on the day on which it receives the Royal Assent.

(k) The *Telecommunications (Interception and Access) Act 1979* was amended by Schedule 1 (items 51–55) only of the *Telecommunications (Transitional Provisions and Consequential Amendments) Act 1997*, subsection 2(2)(d) of which provides as follows:

(2) The following provisions commence on 1 July 1997:

(d) Schedule 1;

(l) The *Telecommunications (Interception and Access) Act 1979* was amended by Schedule 2 only of the *Migration Legislation Amendment Act (No. 1) 1999*, subsection 2(4) of which provides as follows:

(4) Subject to subsection (5), the remaining items of Schedule 1, and Schedule 2, commence on a day to be fixed by Proclamation.

(m) The *Telecommunications (Interception and Access) Act 1979* was amended by Schedule 1 (item 918) only of the *Public Employment (Consequential and*

Authorised Version C2017C00192 registered 03/07/2017

Transitional) Amendment Act 1999, subsections 2(1) and (2) of which provide as follows:

(1) In this Act, ***commencing time*** means the time when the *Public Service Act 1999* commences.

(2) Subject to this section, this Act commences at the commencing time.

(n) The *Telecommunications (Interception and Access) Act 1979* was amended by Schedule 3 (items 1 and 62–81) only of the *Australian Security Intelligence Organisation Legislation Amendment Act 1999*, subsection 2(2) of which provides as follows:

Schedule 3

(2) Subject to subsections (3) to (6), Schedule 3 commences immediately after the commencement of the other Schedules to this Act.

The other Schedules to this Act commenced on 10 December 1999.

(o) Subsection 2(2) of the *Telecommunications (Interception) Legislation Amendment Act 2000* provides as follows:

(2) If items 58 to 64 of Schedule 2 to the *Australian Federal Police Legislation Amendment Act 2000* commence on or after the day on which this Act receives the Royal Assent, then the amendments made by items 2 and 3 of Schedule 3 to this Act commence immediately after the commencement of items 58 to 64 of Schedule 2 to the *Australian Federal Police Legislation Amendment Act 2000*.

Items 58 to 64 of Schedule 2 commenced on 2 July 2000 (*see Gazette* 2000, No. S328).

(p) The *Telecommunications (Interception and Access) Act 1979* was amended by Schedule 47 only of the *Law and Justice Legislation Amendment (Application of Criminal Code) Act 2001*, subsection 2(1)(a) of which provides as follows:

(1) Subject to this section, this Act commences at the later of the following times:

(a) immediately after the commencement of item 15 of Schedule 1 to the *Criminal Code Amendment (Theft, Fraud, Bribery and Related Offences) Act 2000*;

Item 15 commenced on 24 May 2001.

(q) The *Telecommunications (Interception and Access) Act 1979* was amended by Schedule 3 (items 513–515) only of the *Corporations (Repeals, Consequentials and Transitionals) Act 2001*, subsection 2(3) of which provides as follows:

(3) Subject to subsections (4) to (10), Schedule 3 commences, or is taken to have commenced, at the same time as the *Corporations Act 2001*.

Authorised Version C2017C00192 registered 03/07/2017

(r) Subsections 2(1) [item 10] and (4) of the *Australian Crime Commission Establishment Act 2002* provides as follows:

(1) Each provision of this Act specified in column 1 of the table commences, or is taken to have commenced, on the day or at the time specified in column 2 of the table.

Commencement information

Column 1	Column 2	Column 3
Provision(s)	**Commencement**	**Date/Details**
10. Schedule 3, item 17	Immediately after the commencement of section 3 of the *Proceeds of Crime Act 2002*, subject to subsection (4)	1 January 2003

(4) If section 3 of the *Proceeds of Crime Act 2002* commences before 1 January 2003, the provisions covered by items 8, 9 and 10 of the table do not commence at all.

(s) Subsection 2(1) (item 5) of the *Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Act (No. 2) 2004* provides as follows:

(1) Each provision of this Act specified in column 1 of the table commences, or is taken to have commenced, in accordance with column 2 of the table. Any other statement in column 2 has effect according to its terms.

Provision(s)	Commencement	Date/Details
5. Schedule 5, item 9	Immediately after the commencement of item 6 of Schedule 1 to the *Cybercrime Act 2001*.	21 December 2001

(t) Subsection 2(1) (items 5 and 6) of the *Crimes Legislation Amendment (Telecommunications Interception and Other Measures) Act 2005* provides as follows:

(1) Each provision of this Act specified in column 1 of the table commences, or is taken to have commenced, in accordance with column 2 of the table. Any other statement in column 2 has effect according to its terms.

Authorised Version C2017C00192 registered 03/07/2017

Provision(s)	Commencement	Date/Details
5. Schedule 2, item 4	The day on which this Act receives the Royal Assent. However, if section 6 of the *Australian Communications and Media Authority Act 2005* commences before this Act receives the Royal Assent, the provision(s) do not commence at all.	Does not commence
6. Schedule 2, item 5	Immediately after the commencement of section 6 of the *Australian Communications and Media Authority Act 2005*. However, if section 6 of the *Australian Communications and Media Authority Act 2005* commences before this Act receives the Royal Assent, the provision(s) do not commence at all.	Does not commence

(u) Subsection 2(1) (items 5, 7 and 9) of the *Telecommunications (Interception) Amendment Act 2006* provides as follows:

(1) Each provision of this Act specified in column 1 of the table commences, or is taken to have commenced, in accordance with column 2 of the table. Any other statement in column 2 has effect according to its terms.

Provision(s)	Commencement	Date/Details
5. Schedule 6, item 1	Immediately after the commencement of item 10 of Schedule 1 to the *Telecommunications (Interception) Amendment (Stored Communications and Other Measures) Act 2005*.	1 October 2006
7. Schedule 6, item 3	Immediately after the commencement of item 10 of Schedule 1 to the *Telecommunications (Interception) Amendment (Stored Communications and Other Measures) Act 2005*.	1 October 2006
9. Schedule 6, item 8	Immediately after the commencement of section 17 of the *Telecommunications (Interception) Amendment Act 1993*.	1 February 1994

Authorised Version C2017C00192 registered 03/07/2017

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
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
	(1) exp (s 4B(2))
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
s 5AA	ad No 166, 2001

Authorised Version C2017C00192 registered 03/07/2017

Provision affected	How affected
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
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
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
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
s 5E	ad No 40, 2006
s 5EA	ad No 120, 2012
s 5F, 5G	ad No 40, 2006
	am No 177, 2007; No 23, 2008; No 2, 2010
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
s 6AAA	ad No 2, 2010
s 6AA	ad No 40, 2006

Authorised Version C2017C00192 registered 03/07/2017

Endnote 4—Amendment history

Provision affected	How affected
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, 6C	ad No 89, 1987
s 6D	ad No 89, 1987
	am No 120, 1987; No 65, 1988
s 6DA	ad No 160, 1997
	am No 55, 2004; No 40, 2006; No 60, 2015
s 6DB	ad No 40, 2006
	am No 13, 2013; No 60, 2015
s 6DC	ad No 39, 2015
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
s 6EA	ad No 141, 1995
	am No 40, 2006
s 6EAA	ad No 120, 2012
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
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

Authorised Version C2017C00192 registered 03/07/2017

Provision affected	How affected
	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
s 6M	ad No 89, 1987
s 6N	ad No 103, 1993
	am No 9, 2000
s 6P	ad No 63, 2000
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
s 6U	ad No 82, 2016
Chapter 2	
Part II heading	am No 103, 1993
	rep No 40, 2006
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
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

Authorised Version C2017C00192 registered 03/07/2017

Endnote 4—Amendment history

Provision affected	How affected
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; Nos 65 and 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
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
s 9A	ad No 63, 2000
	am No 40, 2006; No 177, 2007; No 23, 2008
s 9B	ad No 63, 2000
	am No 40, 2006

Authorised Version C2017C00192 registered 03/07/2017

Endnote 4—Amendment history

Provision affected	How affected
s 10	am No 43, 1996; No 161, 1999; No 63, 2000; No 128, 2005; No 40, 2006
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
s 11B	ad No 63, 2000
	am No 40, 2006; No 23, 2008; No 50, 2010
s 11C	ad No 63, 2000
	am No 50, 2010
s 11D	ad No 63, 2000
	am No 127, 2004
s 12	am No 102, 1986; No 43, 1996; No 161, 1999; No 63, 2000; No 40, 2006; No 108, 2014
s 13	am No 102, 1986; No 89, 1987; No 103, 1993; No 43, 1996; No 63, 2000; No 40, 2006
s 14	rs No 102, 1986
	am No 89, 1987; No 103, 1993; No 161, 1999; No 63, 2000; No 40, 2006
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
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
s 18	ad No 103, 1993
	am No 161, 1999; No 55, 2001; No 2, 2010; No 108, 2014
	ed C93

Authorised Version C2017C00192 registered 03/07/2017

Endnote 4—Amendment history

Provision affected	How affected
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
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

Authorised Version C2017C00192 registered 03/07/2017

Endnote 4—Amendment history

Provision affected	How affected
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
s 31A–31D	ad No 177, 2007
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
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

Authorised Version C2017C00192 registered 03/07/2017

Endnote 4—Amendment history

Provision affected	How affected
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
s 38A	ad No 82, 2016
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
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
s 45A	ad No 63, 2000
	rep No 40, 2006
	ad No 32, 2009
	rs No 74, 2012

Authorised Version C2017C00192 registered 03/07/2017

Provision affected	How affected
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
s 46A	ad No 63, 2000
	am No 40, 2006; No 23, 2008; No 32, 2009; No 74, 2012; No 82, 2016
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
s 49	ad No 89, 1987
	am No 160, 1997; No 63, 2000; No 67, 2002; No 40, 2006; No 82, 2016
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

Authorised Version C2017C00192 registered 03/07/2017

Endnote 4—Amendment history

Provision affected	How affected
	rs No 40, 2006
s 55	ad No 89, 1987
	am No 11, 1990
	rs No 103, 1993
	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
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
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

Authorised Version C2017C00192 registered 03/07/2017

Provision affected	How affected
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
s 63AA	ad No 141, 1995
	am No 40, 2006
s 63A	ad No 120, 1987
	am No 103, 1993
s 63B	ad No 63, 1989
	am No 141, 1995; No 40, 2006
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
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
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
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
s 68	ad No 89, 1987
	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
s 68A	ad No 7, 2012

Authorised Version C2017C00192 registered 03/07/2017

Endnote 4—Amendment history

Provision affected	How affected
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
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
s 75	ad No 89, 1987
	am No 63, 2000
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
s 78	ad No 89, 1987
	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
s 79A	ad No 2, 2010
Part 2-7	
Part VIII heading	rep No 40, 2006
Part 2-7 heading	ad No 40, 2006

Authorised Version C2017C00192 registered 03/07/2017

Endnote 4—Amendment history

Provision affected	How affected
	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
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
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
s 84	ad No 89, 1987

Authorised Version C2017C00192 registered 03/07/2017

Endnote 4—Amendment history

Provision affected	How affected
	am No 95, 2005; No 40, 2006; No 82, 2016
s 85	ad No 89, 1987
	rs No 82, 2016
s 85A	ad No 82, 2016
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
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

Authorised Version C2017C00192 registered 03/07/2017

Endnote 4—Amendment history

Provision affected	How affected
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
s 103	ad No 89, 1987
	rs No 103, 1993
	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
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

Authorised Version C2017C00192 registered 03/07/2017

Endnote 4—Amendment history

Provision affected	How affected
	am No 103, 1993; No 120, 2012
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
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
s 107Q	ad No 120, 2012

Authorised Version C2017C00192 registered 03/07/2017

Provision affected	How affected
s 107R	ad No 120, 2012
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
Part 3-2	
s 109	ad No 40, 2006
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
s 117	ad No 40, 2006
s 118	ad No 40, 2006

Authorised Version C2017C00192 registered 03/07/2017

Endnote 4—Amendment history

Provision affected	How affected
	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
	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

Authorised Version C2017C00192 registered 03/07/2017

Provision affected	How affected
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
	am No 4, 2011; No 120, 2012
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
s 139A	ad No 194, 2012
	am No 82, 2016; No 95, 2016
s 139B	ad No 82, 2016
	am No 95, 2016
s 139C	ad No 95, 2016
	am No 95, 2016
s 140	ad No 40, 2006
	am No 86, 2006
s 141	ad No 40, 2006
s 142	ad No 40, 2006
	am No 194, 2012; No 82, 2016; No 95, 2016

Authorised Version C2017C00192 registered 03/07/2017

Endnote 4—Amendment history

Provision affected	How affected
s 142A	ad No 120, 2012
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
	am No 194, 2012; No 39, 2015; No 82, 2016; No 95, 2016
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
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

Authorised Version C2017C00192 registered 03/07/2017

Provision affected	How affected
	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
	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
s 163	ad No 40, 2006
	am No 39, 2015
s 163A	am No 7, 2012
Division 3	
s 164	ad No 40, 2006
Part 3-7	
s 165–170	ad No 40, 2006

Authorised Version C2017C00192 registered 03/07/2017

Endnote 4—Amendment history

Provision affected	How affected
Chapter 4	
Chapter 4	ad No 177, 2007
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
Division 4	
s 176A	ad No 39, 2015
	am No 41, 2015
s 177, 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
s 180B	ad No 120, 2012

Authorised Version C2017C00192 registered 03/07/2017

Provision affected	How affected
Subdivision B	
s 180C	ad No 120, 2012
s 180D	ad No 120, 2012
	am No 95, 2016
Subdivision C	
s 180E	ad No 120, 2012
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
s 180K	ad No 39, 2015
s 180L	ad No 39, 2015
s 180M	ad No 39, 2015
s 180N	ad No 39, 2015
s 180P	ad No 39, 2015
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

Authorised Version C2017C00192 registered 03/07/2017

Endnote 4—Amendment history

Provision affected	How affected
Subdivision D	
s 180X	ad No 39, 2015
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
s 182	ad No 177, 2007
	am No 4, 2011; No 120, 2012; No 39, 2015; No 95, 2016
s 182A	ad No 39, 2015
s 182B	ad No 39, 2015
	am No 95, 2016
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
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
s 185E	ad No 39, 2015
s 186	ad No 177, 2007

Authorised Version C2017C00192 registered 03/07/2017

Provision affected	How affected
	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
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
Division 1	
s 187A	ad No 39, 2015
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

Authorised Version C2017C00192 registered 03/07/2017

Endnote 4—Amendment history

Provision affected	How affected
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
Part 5-2	
s 188	ad No 177, 2007
Part 5-3	
Division 1	
s 189–191	ad No 177, 2007
Division 2	
s 192, 193	ad No 177, 2007
Part 5-4	
s 194	ad No 177, 2007
	rep No 4, 2011
s 195, 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–202C	ad No 4, 2011
Part 5-5	
s 203	ad No 177, 2007
	am No 46, 2011

Authorised Version C2017C00192 registered 03/07/2017

Provision affected	How affected
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 208–211	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 108	ad No 89, 1987
Renum s 300	No 40, 2006

Authorised Version C2017C00192 registered 03/07/2017