The Parliament of the Commonwealth of Australia

Review of the Cybercrime Legislation Amendment Bill 2011

Joint Select Committee on Cyber-Safety

August 2011
Canberra

ISBN 978-0-642-79554-0 (Printed version)

ISBN 978-0-642-79555-7 (HTML version)

Contents

Membership of the Committee

Chair	Senator Catryna Bilyk	
Deputy Chair	Mr Alex Hawke MP	
Members	Mr Ed Husic MP	Senator David Bushby
	Ms Nola Marino MP	Senator Scott Ludlam
	Mr Graham Perrett MP	Senator Stephen Parry
	Ms Amanda Rishworth MP	Senator Louise Pratt
	Mr Tony Zappia MP	

Committee Secretariat

Secretary	Mr James Catchpole
Inquiry Secretary	Ms Jane Hearn
Administrative Officers	Ms Heidi Luschtinetz
	Ms Michaela Whyte

Terms of reference

On 23 June 2011, the House of Representatives adopted the report by the House of Representatives Selection Committee entitled *Report No. 26: Consideration of Bills.*

In that report, the Selection Committee determined that the Cybercrime Legislation Amendment Bill 2011 be referred to the Joint Select Committee on Cyber-Safety.

List of abbreviations

AFP	Australian Federal Police
ALRC	Australian Law Reform Commission
ASIO	Australian Security Intelligence Organisation
MA Act	*Mutual Assistance in Criminal Matters Act 1987*
TIA Act	*Telecommunications (Interception and Access) Act 1979*

List of recommendations

4 Mutual Assistance - Stored Communications and Disclosure of Prospective Data to Foreign Countries

Recommendation 1

That the thresholds that apply to the issuing of a stored communication warrant under the *Mutual Assistance in Criminal Matters Act 1987* and the *Telecommunications (Interception and Access) Act 1979* for an investigation or investigative proceeding for a serious foreign offence be the same thresholds as apply for domestic Australian investigations.

Recommendation 2

That the Attorney-General investigate whether the proposed new Part IIIA of the *Mutual Assistance in Criminal Matters Act 1987* may prevent stored communications warrants being available to foreign countries for investigations into child sexual exploitation.

Recommendation 3

That subsection 8(2) of the *Mutual Assistance in Criminal Matters Act 1987* be amended to include an additional discretionary ground to decline a request where the requesting country's arrangements for handling personal information do not offer privacy protection substantially similar to those applying in Australia.

Recommendation 4

That proposed section 180F of the *Telecommunications (Interception and Access) Act 1979* is amended to elaborate more precisely the requirement that the authorising officer consider and weigh the proportionality of the intrusion into privacy against the value of the potential evidence and needs of the investigation.

5 Police Assistance to Foreign Countries – Historic and Existing Telecommunications Data

Recommendation 5

That proposed sections 180A (5) and 180C (2) of the *Telecommunications (Interception and Access) Act 1979* be amended to ensure that, in determining whether a disclosure of telecommunications data to a foreign country is appropriate in all the circumstances, the authorising officer must give consideration to the mandatory and discretionary grounds for refusing a mutual assistance request under existing section 8 of the *Mutual Assistance in Criminal Matters Act 1987.*

Recommendation 6

That the disclosure of telecommunications data to a foreign country in the context of police to police assistance at the investigative stage and in relation to criminal conduct that, if prosecuted, may attract the death penalty, must:

(a) only take place in exceptional circumstances and with the consent of the Attorney-General and the Minister for Home Affairs and Justice; and

(b) each Minister must ensure that such consent is recorded in a register for that purpose.

Recommendation 7

That the Cybercrime Legislation Amendment Bill 2011 be amended to elaborate the conditions of disclosure of historical and existing telecommunications data to foreign countries, including in relation to retention and destruction of the information and an express prohibition on any secondary use by the foreign country.

Recommendation 8

That the Attorney-General investigate the desirability and practicality of a legislative requirement for data subjects to be advised that their communications have been subject to an intercept, stored communications warrant, or telecommunications data disclosure under the *Telecommunications (Interception and Access) Act 1979* once that advice could be given without prejudice to an investigation.

7 Reporting and Oversight

Recommendation 9

That proposed new paragraph 186(1) (ca) of the *Telecommunications (Interception and Access) Act 1979* be amended to require that the Australian Federal Police report to the Minister:

- the number of authorisations for disclosure of telecommunications data to a foreign country;
- identify the specific foreign countries that have received data;
- the number of disclosures made to each of the identified countries; and
- any evidence that disclosed data has been passed on to a third part or parties.

8 Industry Data Handling and Privacy Obligations

Recommendation 10

That the Attorney-General consult initially with the telecommunications industry and then with relevant Ministers, statutory bodies, and public interest groups to clarify and agree on the data handling and protection obligations of carriers and carriage service providers.

Recommendation 11

That the Cybercrime Legislation Amendment Bill 2011 be amended to require carriers and carriage service providers to destroy preserved and stored communications and telecommunications data or a record of that information when that information or record is no longer required for a purpose under the *Telecommunications (Interception and Access) Act 1979* unless it is required for another legitimate business purpose.

Recommendation 12

That the exemption of small Internet Service Providers from the *Privacy Act 1988* as small businesses be reviewed by the Attorney-General with a view to removing the exemption.

9 Industry Implementation Issues

Recommendation 13

That the Attorney-General's Department consult widely with carriers and carriage service providers to ensure that the Cybercrime Legislation Amendment Bill 2011, when enacted, can be implemented in a timely and efficient manner.

1

Introduction

1.1 On 22 June 2011, the House of Representative's Selection Committee referred the Cybercrime Legislation Amendment Bill 2011 (the Bill) to the Joint Select Committee on Cyber-Safety (the Committee) for consideration.[1] Under House of Representatives Standing Order 222, the Selection Committee may refer to the relevant standing or joint committee any bill regarded as 'controversial or requiring further consultation or debate'.

1.2 The main purpose of the Bill is to facilitate Australia's accession to the Council of Europe Convention on Cybercrime (the European Convention). The provisions of the Bill and the European Convention are outlined in Chapter 2 and dealt with in greater detail in the following chapters. It is sufficient to note at this point, that the Bill expands the powers of enforcement agencies and the Australian Security Intelligence Organisation (ASIO), to obtain communications for investigative and security purposes. The Bill will also increase the ability of the Australian Federal Police (AFP) to share data with foreign counterparts.

Conduct of the inquiry

1.3 The Committee agreed to a request by the Attorney-General, the Hon Robert McClelland MP, to table its report in the Parliament by 5 August 2011. By mutual agreement, the reporting date was subsequently extended to 18 August 2011 to allow more time for public submissions.

1.4 The inquiry was advertised electronically and in the national press. Invitations to lodge submissions were sent to all State Premiers and Chief Ministers and to those organisations and individuals likely to have an

---

1 House of Representatives Selection Committee, *Report No. 26: Consideration of bills*, 22 June 2011.

interest in the inquiry. Submissions are listed at Appendix A and are available on the Committee's website at: http://www.aph.gov.au/house/committee/jscc/cybercrime_bill/index.htm

1.5 The Committee received twenty-three submissions and held a public hearing in Canberra on 1 August 2011 followed by an inspection of the AFP High Tech Crime Operations facilities in Barton, Canberra. A list of witnesses who gave evidence at the hearing is at Appendix B.

Previous parliamentary consideration

1.6 In early July 2011, the Senate Standing Committee for the Scrutiny of Bills reviewed the Bill and alerted the Senate to the question of 'whether the bill strikes an appropriate balance of the right to privacy and the policy objectives associated with the implementation of the Convention'.[2] The comments of the Scrutiny of Bills Committee were taken into account during consideration of the Bill.

1.7 Previously, the Parliament has considered both the phenomena of cyber-crime and the European Convention in two separate committee proceedings. In June 2010, the House of Representatives Standing Committee on Communications tabled a report of its inquiry into cybercrime.[3] Among other things, the Committee recommended that the Attorney-General, in consultation with state and territory counterparts, move expeditiously to accede to the Convention on Cybercrime.[4] The Committee also said any changes to Australian legislation should also be consistent with its obligations under the International Covenant on Civil and Political Rights.[5]

1.8 In April 2011, the Joint Standing Committee on Treaties considered Australia's proposed accession to the European Convention and also made relevant comments on issues that now arise under the Bill.[6] While the Treaties Committee supported binding treaty action; it also took note of the importance of their being adequate safeguards to protect privacy and civil liberties.[7]

---

2 Senate Standing Committee for the Scrutiny of Bills, *Alert Digest No.7 of 2011*, 6 July 2011, p. 4.

3 House of Representatives Standing Committee on Communications, *Hackers, Fraudsters and Botnets: Tackling the Problem of Cyber Crime*, June 2010, Canberra.

4 Standing Committee on Communications, *Hackers, Fraudsters and Botnets*, p. 122.

5 Standing Committee on Communications, *Hackers, Fraudsters and Botnets*, p. 121.

6 Joint Standing Committee on Treaties, *Report 116*, April 2011, Canberra; Chapter 11, pp. 79-91.

7 Joint Standing Committee on Treaties, *Report 116*, pp. 86-92.

1.9 Finally, it should be noted that this Bill has been introduced into Parliament at a time of debate about a proposed data retention scheme for electronic communications that was the subject of an Inquiry by the Senate Environment and Communications References Committee into the adequacy of privacy protections for Australian citizens online.[8] Neither the European Convention nor the Bill seeks to implement a communications retention scheme.

8 Senate Environment and Communications References Committee, *The adequacy of protections for the privacy of Australians online*, April 2011, Canberra.

2

Outline of the European Convention on Cybercrime and the Cybercrime Bill

Introduction

2.1 As noted in Chapter 1, the Cybercrime Legislation Amendment Bill 2011 (the Bill) contains provisions intended, among other things, to facilitate Australia's accession to the Council of Europe Convention on Cybercrime (the European Convention). In September 2010, Australia was formally invited by the Council of Europe to accede to the European Convention and, the provisions of the Bill are intended to complete the domestic legislative work required prior to acceding to binding treaty obligations.

2.2 This section outlines some of key aspects of the European Convention and the Bill.

European Convention on Cybercrime

2.3 The European Convention is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security.[1] The main objective of the European Convention, set out in the preamble, is to pursue a common criminal policy aimed at the protection of society against

1 Council of Europe, Convention on Cybercrime, ETS No. 185.

cybercrime, especially by adopting appropriate legislation and fostering international co-operation.[2]

2.4 The European Convention was developed by Members of the Council of Europe, with the participation of both European and non-European states. At the time of writing, 30 member states of the Council of Europe and one non member state (the United States of America) have acceded to the European Convention. Another 16 nations (both Council of Europe and other) have signed but not ratified the Convention.[3]

2.5 In summary, the European Convention requires States parties to:

- create a range of computer offences (illegal access, illegal interception, data interference, system interference) and computer enabled offences relating to forgery, fraud, child pornography, and infringement of copyright and intellectual property (Chapter II, Articles 2-13);
- establish powers and procedures to allow investigation of computer offences as set out in the European Convention, other computer enabled crime, and the collection of electronic evidence of any criminal offence (Chapter II, Articles 14-21); and
- co-operate with other Convention signatory countries (States parties) in the investigation and proceedings relating to computer offences, and the collection of electronic evidence of any criminal offence (Chapter III, Articles 23-35);

2.6 The European Convention contains several express limitations and assumptions that :

- limits the scope of procedural powers by requiring that such powers are 'for the purpose of specific criminal investigations and proceedings' (Article 14.1). The Explanatory Report to the European Convention reminds States parties that the power and procedures of the European Convention are limited to use for 'an investigation in a particular case';[4]
- permits States parties to limit the range of offences for which assistance is to be given to a foreign country to ensure such measures are proportionate and do not unnecessarily intrude into personal privacy.

---

2 The Convention has been supplemented by an Additional Protocol making any publication of racist and xenophobic propaganda via computer networks a criminal offence.

3 Signatories to the European Convention, <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG>, viewed 4 August 2011.

4 *Explanatory Report, Convention on Cybercrime,* paragraph 152, p. 25.

For example, a country may limit mutual assistance to serious offences rather than all offences (Article 33);

- requires that all powers and procedures must be subject to conditions and safeguards to ensure the protection of human rights (Article 15). This includes judicial or other independent supervision, the need for grounds to justify an application under the European Convention, and a limitation of the scope and the duration of the particular power or procedure under the Convention (Article 15.1);
- requires States parties to adhere to common standards or minimum safeguards, including those pursuant to obligations under the European Convention for the Protection of Human Rights and Fundamental Freedoms. States parties from other regions of the world are to adhere to applicable human rights instruments (such as the International Covenant on Civil and Political Rights);[5] and
- requires that powers and procedures shall "incorporate the principle of proportionality", and, among other things, the right against self-incrimination, access to legal privileges, and the specificity of individuals or places which are the object of European Convention measures.[6]

Cybercrime Legislation Amendment Bill 2011

2.7 The Bill is described as a 'Bill for an Act to implement the Convention and for other purposes'. In summary, the Bill:

- requires carriers and carriage service providers to preserve the stored communications and telecommunications data for specific persons when requested by certain domestic agencies or when requested by Australian Federal Police on behalf of certain foreign countries;
- ensures Australian agencies are able to obtain and disclose telecommunications data and stored communications for the purposes of a foreign investigation;
- provides for the extraterritorial operation of certain offences in the *Telecommunications (Interception and Access) Act 1979* (TIA Act);

5 *Explanatory Report to the Convention*, paragraph 145, p. 24; see also advice Mr A Seger, Head of Economic Crime Division, Directorate General of Human Rights and Legal Affairs, Council of Europe, *Submission 4*, p. 2.

6 *Explanatory Report to the Convention*, paragraph 146, p. 24.

- removes the constitutional restriction from the computer crime offences in the *Criminal Code Act 1995* so they have adequate scope;
- creates confidentiality requirements in relation to authorisations to disclose telecommunications data.[7]

2.8 The Bill achieves these objectives by amending the following Acts:

- *Telecommunications Act 1997*;
- *Telecommunications (Interception and Access) Act 1979*;
- *Mutual Assistance in Criminal Matters Act 1987*;
- *Criminal Code Act 1995*.

Telecommunications Act 1997

2.9 The *Telecommunications Act 1997* regulates the telecommunications industry.

2.10 Part 13 of the *Telecommunications Act 1997*, makes it an offence for a carrier or carrier service provider and its employees to use or disclose any information or document which comes into its possession in the course of its business, where the information relates to:

- the contents or substance of a communication carried by the carrier or carriage service provider, whether the communication is delivered or not; or
- carriage services supplied, or intended to be supplied, by the carrier or carriage service provider; or
- the affairs or personal particulars of another person.

2.11 The exceptions to the prohibition on disclosure of information include:

- where the disclosure is reasonably necessary for the enforcement of the criminal law, enforcement of a law imposing a pecuniary penalty, and protection of public revenue;
- where the disclosure is made to Australian Security Intelligence Organisation (ASIO) for the performance of its functions;
- where the disclosure is required or is otherwise authorised under a warrant or under law.

7 *Explanatory Memorandum,* Cybercrime Legislation Amendment Bill 2011, p. 1.

2.12 The *Telecommunications Act 1997* imposes an obligation on carriers and carriage services providers to provide reasonable assistance to enforcement agencies necessary to enforce the criminal law and intelligence agencies for security purposes.[8]

Telecommunications (Interception and Access) Act 1979

2.13 The *Telecommunications (Interception and Access) Act 1979* (TIA Act) works in conjunction with the *Telecommunications Act 1997*, to prohibit the interception, collection, or disclosure of communications unless authorised under the Act.

2.14 The TIA Act currently contains three distinct regimes that regulate the use of powers depending on the sensitivity of the data and the purpose for which it is sought:

- interception warrants allow for the real-time copying or recording of information passing over a telecommunications system (chapter 2);
- stored communications warrants allow access to communications stored on the equipment of the carrier (chapter 3); and
- non warrant based authorisations allow for the disclosure of information about communications but not the communications themselves (chapter 4).

2.15 The TIA Act created the position of the Communications Access Coordinator which is located within the Attorney-General's Department, and is the first point of contact for the telecommunications industry, law enforcement agencies and national security agencies under the Act.

Mutual Assistance in Criminal Matters Act 1987

2.16 The *Mutual Assistance in Criminal Matters Act 1987* (MA Act) regulates the granting of international assistance by Australia in relation to criminal matters in response to a request from a foreign country.[9]

2.17 Under the MA Act, the Attorney-General must refuse assistance to foreign countries in six specific circumstances. These include where the offence is a political offence, the person has already been acquitted or pardoned

8 Section 313 of the *Telecommunications Act 1997*.

9 The forms of assistance include, for example, the taking of evidence, production of documents, search and seizure orders, the forfeiture or confiscation of property, and the recovery of pecuniary penalties; see section 5, *Mutual Assistance in Criminal Matters Act 1987*, 'Objects of the Act.'

(double jeopardy) or because providing assistance would prejudice the sovereignty, security or national interest of Australia (paragraphs 8 (1) (a)–(f)).

2.18 Assistance may also be refused on a number of other grounds, including :

- where the conduct is not an offence in Australia;
- where if it occurred in Australia the offence could not be prosecuted because of lapse of time or other reasons;
- would prejudice an Australian investigation, or
- would impose an excessive burden on Commonwealth, state or territory resources (subsection 8 (2)).

Death penalty

2.19 The Attorney-General must refuse assistance to a foreign country if the offence carries the death penalty in that country, unless he or she is of the opinion that special circumstances of the case warrant the provision of assistance (section 8 (1A) of the MA Act). Under section 8(1B), the Attorney-General may also refuse assistance where the assistance may result in the death penalty being imposed, and, having regard to the interests of international cooperation decided that assistance should not be granted.

Criminal Code Act 1995

2.20 The *Criminal Code Act 1995* provides the general principles of criminal responsibility that apply in the prosecution of all offences against laws of the Commonwealth. It sets out the elements of offences and what is required to establish guilt in respect of offences, including as to the required burden of proof. Part 10.7 of the Criminal Code details computer offenses, including unauthorised modification or impairment in, to, or from a computer.

3

Domestic and Foreign Preservation Notices

Introduction

3.1 This chapter deals with provision of the Cybercrime Legislation Amendment Bill 2011 (the Bill) that introduce 'preservation notices', a new provisional measure available to enforcement agencies and Australian Security Intelligence Organisation (ASIO) to prevent the destruction of communications.

3.2 The relevant articles of the Council of Europe Convention on Cybercrime (European Convention) are set out followed by the provisions of the Bill and associated commentary.

European Convention on Cybercrime

3.3 Article 16 requires States parties to provide for the expedited preservation of 'stored computer data' for domestic agencies. Computer data is defined under Article 1(b), as data in an electronic or other form that can be directly processed by a computer system. It includes both content and traffic data.

3.4 Under Article 16, a States party has an obligation to enable domestic agencies to order the preservation of specified computer data, including traffic data that has been stored by means of a computer system, for up to 90 days. In particular, preservation is to be made available where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.

3.5 Article 17 requires that traffic data preserved under Article 16 (as distinct from content data), must be available for disclosure to allow identification of service providers and the path through which the communication was transmitted.

3.6 Article 29 requires State parties to make available to foreign law enforcement agencies the expedited preservation of stored computer data for the investigation of a serious foreign criminal offence. The Explanatory Report emphasises that under Article 29, the preservation of existing stored data is a provisional measure intended to prevent the destruction of evidence in the time it takes to prepare, transmit and execute a request for mutual assistance to obtain the data.[1]

3.7 A request for preservation under Article 29 may be refused (except for Convention computer offences) if dual criminality cannot be fulfilled; the offence is considered to be a political offence or connected to a political offence; or execution of the request is likely to prejudice its sovereignty, security or *ordre public* or other essential interests (Articles 29(4), (5),(6)).[2]

Cybercrime Legislation Amendment Bill 2011

Domestic preservation notices

3.8 Schedule 1 of the Bill amends the *Telecommunications Act 1997* and the *Telecommunications (Interception and Access) Act 1979* (TIA Act). The amendments insert new Part 3 – 1A into Chapter 3 of the TIA Act to create a regime for preserving stored communications. Chapter 3 is renamed *Preserving and Accessing Stored Communications.*

3.9 New Part 3 – 1A Division *2* will make available:

- a domestic historic preservation notice that requires a carrier or carriage service provider to preserve communications it holds in relation to a specified individual or a specified telecommunications service from the time of receipt of the notice until the end of that day (proposed paragraph 107H(1)(i)); and

1 *Explanatory Report to the Convention on Cybercrime.*

2 A country that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or disclosure of stored data may reserve the right to refuse a preservation request for preservation in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled. There is no exception for computer offences enshrined in Articles 2 to 11 of the Convention.

- a domestic ongoing preservation notice that requires a carrier or carriage service provider to preserve communications on an ongoing basis in relation to a specified individual or a specified telecommunications service commencing from the time of receipt of the notice for up to 29 days (proposed paragraph 107H(1)(ii)).

Period in force

3.10 The domestic preservation notices remain in force until revoked or a period of 90 days elapses. The 90 day period is intended to ensure that communications preserved under the notice is maintained and available to be accessed under a warrant (proposed paragraph 107(b) (i) (ii)).

3.11 If the agency obtains an intercept warrant, the preservation notice remains in force the duration of the warrant, which may be less than 90 days (proposed paragraph 107K (b) (iii)).[3] In the case of an intercept warrant by ASIO, the preservation notice remains in force for 5 days after the warrant is issued (proposed paragraph 107K (b) (IV)).

Enforcement agencies and interception agencies

3.12 Both historic and ongoing preservation notices are available to a wide range of agencies, but these vary according whether the preservation of communications is on an ongoing or historic basis. Ongoing preservation of communications is considered more intrusive and is limited to 'interception agencies' (see below).

3.13 A domestic historic preservation notice may be issued by an 'enforcement agency' or ASIO. Under the TIA Act, an enforcement agency is an agency that can apply for a stored communication warrant (section 5 of the TIA Act). ASIO may access stored communications via an interception warrant. There are currently seventeen enforcement agencies in Australia, including, for example, Federal and State police forces, anti-corruption and police integrity bodies, the Australian Customs Service and CrimTrac.

3.14 An enforcement agency also includes bodies that administer a law imposing a pecuniary penalty; or relate to the protection of the public purses. These would include, for example, the Australian Securities and Investment Commission. The definition and list of enforcement agencies is set in Appendix C to this report.

---

3 An intercept warrant may be issued for up to 90 days, except in the case of a warrant to intercept the communications of a third person with whom the suspect may communicate which is limited to 45 days.

3.15 On the other hand, a domestic ongoing preservation notice is available only to an 'interception agency'. An interception agency under the TIA Act includes ASIO, Federal and State police forces and State and Federal anti-corruption and integrity commissions (section 5 of the TIA Act). A domestic ongoing preservation notice is not available to the Australian Customs Service or CrimTrac or bodies responsible for administering law that impose a pecuniary penalty or for the protection of the public revenue. A complete list of interception agencies is set out in Appendix D to this report.

Thresholds - enforcement agencies

3.16 Under proposed section 107J, an historic or ongoing domestic preservation notice may be issued where the agency:

- is investigating a 'serious contravention'; and
- has reasonable grounds for suspecting the communication does or might exist, and might assist in the investigation; and
- has formed an intention to access the communications with a 'stored communication warrant' or an 'interception warrant' (Part 2-5 of the TIA Act) if the data would be likely to assist with the investigation in the future.

3.17 A serious contravention is an offence under Commonwealth, State or Territory law that is a 'serious offence' or an offence punishable by at least three year maximum imprisonment, a fine of at least 180 penalty units (natural persons) or 900 penalty units. (section 5E of the TIA Act).[4]

Thresholds - ASIO

3.18 The Bill extends the power to issue ongoing and historic domestic preservation notices to ASIO for intelligence gathering purposes where:

- there are reasonable grounds for suspecting the communication(s) does or might exist, and might assist in gather intelligence relating to security;[5] and
- ASIO has formed an intention to apply for access to the stored communication by requesting an interception warrant under Part 2-2 of the TIA Act.

4 A contravention is one that has or is being committed, or is suspected on reasonably grounds of having been committed or being committed or likely to be committed.

5 'Security' as defined in section 4 of the *Australian Security Intelligence Organisation Act 1979.*

3.19 To obtain an interception warrant under Part 2-2 the Director General of Security must make a request to the Attorney-General.[6]

Revocation

3.20 A domestic preservation notice may be revoked at any time and must be revoked if the preconditions that triggered the power no longer exist. For example, if the investigation ceases or the agency ceases to have reasonable grounds for believing the communications exist or might exist in respect of the individual or service. It follows that in these circumstances the agency would no longer hold an intention to access the material via a relevant warrant.

3.21 A revocation is only effective if it is given by the issuing agency to the carrier in writing (proposed subsection 107L (3)).

3.22 Equivalent provisions apply to ASIO for revocation of a preservation notice to collect data for a security purpose (proposed subsection 107L (1) (2)).

Foreign preservation notices

3.23 Schedule 1 of the Bill also proposes to amend the TIA Act to create a foreign preservation notice to implement Article 29 of the European Convention.

3.24 Proposed sections 107N to 107S will introduce a new regime that requires the Australian Federal Police (AFP) to issue a foreign preservation notice in relation to a particular person or telecommunication service on receipt of a request from a foreign country (proposed sections 107N, 107P).

3.25 The AFP has no discretion to refuse such a request but the content may only be disclosed in response to a formal mutual assistance request that has been agreed to by the Attorney General.

3.26 The obligation applies to the AFP only. ASIO has no obligation or authority to issue a preservation notice on behalf of a foreign country.

3.27 The carrier(s) or carriage service provider(s) must preserve all 'stored communications' held at the time of the notice received until the end of that day.

---

6 Section 109 of the *Telecommunications (Interception and Access) Act 1979* (TIA Act) extends the Part 2-2 Interception Warrant regime to include access to stored communication if the warrant would have authorised interception if the data was still passing over the computer system.

Threshold

3.28 To trigger the AFP's obligation to issue the notice to a carrier or carriage service provider in Australia, the foreign country must:

- intend to submit a formal mutual assistance request under section 15B(d) of the *Mutual Assistance in Criminal Matters Act 1987*;
- indicate that the communications relate to an identified person or telecommunications service;
- indicate that the communications are held by a carrier;
- confirm that the request relates to an investigation or an investigative proceeding for a serious criminal offence under the law of that country (proposed subsection 107P (1)).

3.29 The request must be in writing, but it may be by facsimile or email. The written request must specify the name of the authority, the serious foreign criminal offence, identify the stored communication to be preserved and its relationship to the offence; identify (if possible) the carrier, the telecommunications service (if possible) and the reasons for the request. The request must also state an intention by the foreign country to make a formal request for access to the stored communications (proposed section 107P).

Revocation

3.30 The AFP must revoke a foreign preservation notice in writing by the third day after:

- 180 days from the day the carrier received the notice have elapsed and no formal mutual assistance request is made by the requesting country; or
- the Attorney General refuses the mutual assistance request; or
- the country withdraws the mutual assistance request (proposed section 107R).

Commentary

Distinction between content and traffic data

3.31 The Australian Privacy Foundation pointed to the distinction between the substance of communications and traffic data in the Convention.[7] The Foundation was concerned that the Bill fails to make this distinction in the preservation regime: [8]

> As currently drafted, the Bill does not specifically differentiate between traffic and content data and instead merely refers to "stored communications" which is not defined. The use of this phrase is unnecessarily broad and increases the scope for unwarranted privacy intrusions into personal communications where preservation and disclosure of traffic data alone could be sufficient in terms of an ongoing investigation.[9]

3.32 The TIA Act uses the terminology of 'communication' and 'stored communication' as follows:

- 'communication' - a conversation and a message in a variety of forms including, for example, speech, data, text, visual images, video, signal and so forth. It includes email, text, and recorded voice mail; and
- 'stored communication' - a communication that is not passing over the telecommunications system; is in the possession and control of the carrier and cannot be accessed by anyone other than the sender or recipient without the assistance of the carrier.[10]

3.33 These definitions clearly suggest it is the intention of the Bill, that the preservation notices (domestic and foreign) preserve the substance of the communication. In the case of an ongoing domestic preservation notice, this includes the preservation of communications for up to 30 days (see Interception below).

3.34 The European Convention explicitly defines 'traffic data' in some detail, subjects it to a different regime, and allows States parties to differentiate traffic data from content in accordance with their domestic privacy

---

7 Australian Privacy Foundation, *Submission 16*, pp.3-4.

8 Australian Privacy Foundation, *Submission 16*, p. 4.

9 Australian Privacy Foundation, *Submission 16*, p. 4

10 Section 5 of the TIA Act.

sensitivities.[11] The Explanatory Report explains that the Convention makes this distinction because the ephemeral nature of traffic data makes its expeditious preservation necessary, and the ordinary procedures for collection and disclosure of computer data may be insufficient.[12]

3.35 It is common ground that traffic data can provide significant evidence of criminal behaviour, especially in relation to computer offences.[13] It provides the means to trace the source of a communication and is a starting point to collecting further evidence of the offence. The Convention recognises that States parties may differentiate between traffic and content data, and that substantive criteria and procedure to apply the investigative powers may vary according to the sensitivity of the data.[14]

3.36 The Australian Privacy Foundation advised that, in the context of Australia, telecommunications and interception law already distinguishes between content and other data, with different thresholds, tests and controls for collection and recording.[15] The three distinct regimes that provide for interception, access to stored communications, and non-warrant based authorisations are referred to in Chapter 2.

3.37 The Australian Privacy Foundation submitted that the Bill:

- should clearly distinguish between traffic and content data for the purposes of preservation and any subsequent disclosure; and
- ensure higher threshold tests and stricter controls that currently apply to activities that involve content data are not compromised by the proposed preservation and access regime.[16]

---

11 Article 1(d) defines 'traffic data' and lists exhaustively the categories of traffic data that are treated by a specific regime in the Convention: the origin of a communication, its destination, route, time (GMT), date, size, duration and type of underlying service. Not all of these categories will always be technically available, capable of being produced by a service provider, or necessary for a particular criminal investigation. The "origin" refers to a telephone number, Internet Protocol (IP) address, or similar identification of a communications facility to which a service provider renders services. The "destination" refers to a comparable indication of a communications facility to which communications are transmitted. The term "type of underlying service" refers to the type of service that is being used within the network, e.g., file transfer, electronic mail, or instant messaging.

12 *Explanatory Report to the Convention*, para. 29, p. 6.

13 Australian Privacy Foundation, *Submission 16*, p. 4; *Explanatory Report to the Convention on Cybercrime*, para. 29, p. 6.

14 Article 15 of the Convention, *Explanatory Report*, para. 31, p. 6.

15 Australian Privacy Foundation, *Submission 16*, p. 4

16 Australian Privacy Foundation, *Submission 16*, p. 4.

Distinction between ongoing preservation and interception

3.38 While acknowledging the purpose and benefit of the amendments, the Ombudsman expressed several concerns about the practical operation of the preservation notice scheme.

3.39 In particular, the Ombudsman drew attention to the ongoing domestic preservation notice, which requires carriers to preserve stored communications for 29 days. It was submitted that this enables an agency to obtain communications passing over a carrier's system for a period into the future and effectively amounts to a telecommunications interception, which is regulated under existing Part 2 of the TIA Act.[17]

3.40 In addition, although an ongoing preservation notice in relation to the same person or service can only be issued one at a time, it does not prevent an agency from issuing another ongoing preservation notice. This aspect of the Bill can potentially lead to ongoing preservation of stored communications for a long period of time. The Ombudsman concluded that, again, this effectively amounts to a telecommunications interception, which is regulated by a separate Part 2-5 of the TIA Act.[18]

3.41 The European Convention requires the preservation of stored computer data, but it does not provide for ongoing collection of content data.[19] Under the Convention, preservation measures are to apply to 'computer data that has been stored by means of a computer system'. This presupposes that the data already exists, has already been collected and is stored:

> The articles therefore provide only for the power to require preservation of existing stored data, pending subsequent disclosure of the data pursuant to other legal powers, in relation to specific criminal investigations or proceedings.[20]

3.42 The Explanatory Report to the Convention emphasises that:

> The measures in Article 16 and 17 apply to stored data that has already been collected and retained by data-holders, such as service providers. They do not apply to the real time collection and retention of future traffic data or to real time access to the content

17 Commonwealth Ombudsman, *Submission 15*, p.3; Australian Privacy Foundation, *Submission 15*, p. 3.

18 Commonwealth Ombudsman, *Submission 15*, p. 2.

19 Commonwealth Ombudsman, *Submission 15*, p.2

20 Privacy Foundation of Australia, *Submission 16*, p. 3.

of communications. These issues are addressed in Title 5 (real time collection of computer data).[21]

3.43 The distinction between preservation of stored computer data and the ongoing collection of data, especially content data, is further reinforced by Article 21 of the Convention. Article 21 explicitly states that the interception of content data should only occur in relation to serious domestic offences.

Threshold – serious offence and serious contravention

3.44 The Bill proposes that the threshold for a domestic historic or ongoing preservation notice will be that the agency is investigating a 'serious contravention' of Australian law. Under the TIA Act a serious contravention is defined as encompassing a 'serious offence', national security, or an offence punishable by a maximum of 3 years imprisonment, 180 penalty units for an individual or 900 penalty units for a body corporate.[22]

3.45 Under the Bill, the power to issue an ongoing preservation notice will be limited to the narrower group of 'interception agencies' whereas a notice to preserve historic data will be available to the wider range of 'enforcement agencies'. This differentiation appears to reflect recognition that the collection of future private communications over a thirty day period is significant and intrusive and should be subject to restriction.

3.46 An interception agency will then have access to the preserved communications for the investigation of a 'serious contravention' via a stored communications warrant. A stored communications warrant authorises access to a stored communication (i.e. already held on the carriers equipment), but not collection or interception.[23] In contrast, an interception agency may only obtain an interception warrant for real time copying or recording of future transmissions for the investigation of a serious offence or for a national security purpose (Part 2-5 of the TIA Act).

3.47 It has been suggested that, in practice, the ongoing preservation notice regime significantly expands the power of police and other crime, anti-corruption and integrity agencies to gain access to a larger volume of

21 *Explanatory Report to the Convention*, para. 149, p.25.

22 Section 5E of the TIA Act.; A serious contravention is one that has been committed, or is suspected on reasonable grounds of having been committed, or of being likely to be committed.

23 Section 117 of the TIA Act.

content data for a wider range of activity than would otherwise be available under the interception regime.

3.48 In the case of ASIO, an ongoing preservation notice for communications relating to security remains subject to a separate interception regime under Part 2-2 of the TIA Act (that also provides access to stored communications).

Foreign countries

3.49 Several submitters made the point that the Bill did not propose to limit the new powers and procedures to foreign countries that are parties to the European Convention. Where the mutual assistance law applies, the scope of 'foreign country' will run in parallel to Australian existing mutual assistance arrangements. In the police-to-police assistance context, this restraint is not present. For the purpose of a foreign preservation notice, these notices are available at large and without the discretion to refuse assistance provided to the AFP.[24]

3.50 The Australian Privacy Foundation, for example, pointed out that only four non-Council of Europe countries have signed the Convention and that of those, only the United States of America has ratified it.[25]

> This means that the vast majority of countries that might seek preservation and/or disclosures under the proposed provisions of the TIA Act would not be party to the Convention and its conditions and safeguards.[26]

Committee View

3.51 The Committee understands that the preservation mechanism is intended as an interim measure, to prevent the destruction of potentially useful evidence until a warrant for a stored communication can be obtained.

3.52 It has been argued that an ongoing preservation notice for up to thirty days is not required by the European Convention and effectively amounts to an interception that would otherwise be regulated under Chapter 2 of the TIA Act. However, the Committee has been assured that agencies will

24 Australian Privacy Foundation, *Submission 16*, p. 7.

25 Australian Privacy Foundation, *Submission 16*, p. 7.

26 Australian Privacy Foundation, *Submission 16*, p. 7.

not have access to this material unless and until a stored communications warrant is obtained.

3.53 In the case or a foreign preservation notice, the preservation will last only for up to a 24 hour period. Access is then regulated through the mutual assistance regime and an independently supervised application for a stored communication warrant. This provides an important safeguard against access that may otherwise be inconsistent with Australian values.

4

Mutual Assistance - Stored Communications and Disclosure of Prospective Data to Foreign Countries

Introduction

4.1 This chapter discusses aspect of the Cybercrime Legislation Amendment Bill 2011 (the Bill) intended to facilitate:

- access by a foreign country to stored communications for a foreign investigation or investigative proceeding; and
- authorise the disclosure of prospective communications to a foreign country.

European Convention on Cybercrime

4.2 The Council of Europe Convention on Cybercrime (European Convention) requires States parties to cooperate and assist each other in identifying perpetrators and preserving vulnerable traffic data relevant to the foreign criminal investigation:

- Article 30(1) requires 'expeditious disclosure' of 'sufficient traffic data' to identify a service provider and the path of transmission in another State discovered while responding to a request to preserve data (see foreign preservation notice). Traffic data may be withheld if the request concerns a 'political offence' or is likely to 'prejudice its sovereignty, security, *ordre public* or other essential interests' (Art 30(2));

- Article 33 requires mutual assistance in the real time collection of traffic data. The purpose of real time collection of 'traffic data' is to trace the source or destination of computer communications (thus, assisting in identifying criminals);[1]
- Article 31 requires mutual assistance to 'access stored data' in their territory where there are grounds to believe the data is particularly vulnerable to loss or modification.

Cybercrime Legislation Amendment Bill 2011

4.3 Schedule 2 Part 1 of the Bill proposes to amend the *Mutual Assistance in Criminal Matters Act 1987* (MA Act) and the *Telecommunications (Interception and Access) Act 1979* (TIA Act) to enable the Federal and State police forces to:

- apply for a warrant to access stored communication (content data) for a foreign law enforcement purpose where the country has made a formal request for assistance that has been granted by the Attorney-General; and
- authorise the disclosure of 'prospective telecommunication data' for a foreign law enforcement purpose where the country has made a formal request for assistance that has been granted by the Attorney-General.

Stored Communications Warrants

4.4 Under the existing MA Act, covertly accessed stored communication obtained during an Australian investigation may be disclosed to a foreign country under a 'take evidence' or 'production order' issued by a magistrate (s.13). The Attorney-General's Department argues that this mechanism can be time-consuming, and is limited to information which has already been obtained in the course of an Australian investigation.[2]

4.5 The Bill proposes to insert a new section 15B into the MA Act to enable the Attorney-General to authorise the Australian Federal Police (AFP) or State

1 Investigators are unable to be sure they can trace a communication to its source following the trail through records of prior transmission because key traffic data may be automatically deleted by a service provider in the chain of transmission before it could be preserved; see *Explanatory Report to the Convention on Cybercrime*, para. 294, p. 54.

2 *Explanatory Memorandum*, Cybercrime Legislation Amendment Bill 2011, p. 19.

police to apply under the TIA Act to an 'issuing authority' for a 'stored communication warrant' in response to a request from a foreign country.[3]

Thresholds

4.6 The preconditions to an exercise of the Attorney-General's discretion are that the he or she must be satisfied that:

- a criminal investigation or investigative proceeding has commenced in the requesting country into an offence, which is 'a serious criminal offence' under the law of that country; and
- there are reasonable grounds for believing the carrier holds the stored communication.

4.7 A serious criminal offence is defined as an offence punishable by a maximum three years imprisonment, life, death or a fine equivalent to 900 penalty units (currently $10,000). [4] This penalty threshold is modelled on the threshold for a stored communication warrant for a domestic offence.

Safeguards

4.8 The Bill also amends the TIA Act to require that the issuing authority must be satisfied that:

- the information would be likely to be obtained under the warrant ,
- would be likely to assist in the investigation of a serious foreign offence to which the mutual assistance application relates; and
- is related to the particular person involved, including a victim.[5]

4.9 The issuing authority must also 'have regard' to:

- how much the privacy of any person(s) is likely to be interfered with by the accessing of the stored communications;

---

3 An 'issuing authority' under section 6DB of the *Telecommunications (Intercept and Access) Act 1979* (TIA Act) includes a Federal Court judge, a federal magistrate, a member, a legally qualified senior member or Deputy President of the Administrative Appeals Tribunal enrolled for at least five years.

4 The Attorney-General must have reasonable grounds to believe the stored communications are relevant to a foreign investigation or investigative proceeding. *Explanatory Memorandum*, p. 7.

5 Proposed subparagraph 116(1) (d) (ii)) of the TIA Act.

- the gravity of the conduct constituting the 'serious foreign contravention'; and
- how much the information would be likely to assist the investigation to the extent that this is possible to determine from the information obtained from the foreign country to which the application relates.[6]

Conditions of Disclosure

4.10 Proposed section 142A of the TIA Act, provides that a person may only communicate information, obtained through the execution of a warrant, to the foreign country to subject to the following conditions:

- that the information will only be used for the purposes for which the foreign country requested the information;
- that any document or other thing containing the information will be destroyed when it is no longer required for those purposes; and
- any other condition determined, in writing, by the Attorney-General.

Commentary

4.11 The Law Council of Australia identified three primary concerns with the access and disclosure of stored communications for a foreign country.[7] The Australian Bar Association endorsed the Council's submission and several other submitters echoed the same concerns.[8] The concerns relate to:

- the threshold for granting a stored communications warrant;
- privacy safeguards in proposed new section 180F; and
- conditions of disclosure.

6 Proposed subsection 116(2A) of the TIA Act.

7 Law Council of Australia, *Submission 5*, p. 4.

8 Australian Bar Association, *Submission 9*. See also NSW Office of the Privacy Commissioner, *Submission 22*; Electronic Frontiers Australia, *Submission 8*; NSW Council of Civil Liberties, *Submission 21*; Queensland Council of Civil Liberties, *Submission 12*.

Thresholds – justification by foreign country

4.12 The Law Council of Australia argued that a foreign law enforcement authority should not be able to access stored communications that would not be available to domestic authorities.[9]

4.13 In the context of a domestic investigation, an issuing authority must consider:

- how much the information that might be obtained under a warrant would be likely to assist the investigation;[10]
- the extent to which other methods of investigation have been used or are available;
- the efficacy of such other methods or the extent to which alternative methods would be likely to prejudice the investigation through delay or some other reason.[11]

4.14 The Bill proposes to lower the threshold, requiring that the value of the stored communication is to be assessed only to the extent that the information provided by the requesting country allows for such an evaluation. There is no requirement that a foreign country justify the use of a stored communications compared to other less intrusive methods.

4.15 The Law Council of Australia argues that, if foreign agencies want to be able to employ intrusive police powers, they ought to be required to provide sufficient information on the merits of their request, including the likely value of the evidence or information sought.[12]

Threshold - dual criminality

4.16 The Bill restricts access to stored communications only to assist in the investigation of a 'serious foreign offence'. The definition of 'serious offence' in the Bill is the same for a domestic offence and a foreign offence.

4.17 The Explanatory Memorandum to the Bill expresses an intention to only share information where there is a comparable offence in Australia:

> A similar penalty threshold will ensure that stored communications warrants for foreign offences will only be able to

9 Law Council of Australia, *Submission 5*, p. 5.

10 Paragraph 116(2)(c) of the TIA Act.

11 Paragraph 116(2)(d-f) of the TIA Act.

12 Law Council of Australia, *Submission 5*, p. 5.

be issued where a warrant for a domestic investigation would also be able to be issued.[13]

4.18 Further, the reporting requirements for mutual assistance applications under proposed paragraph 162(1)(d) of the TIA Act will require, among other things, reporting of the offence (if any), under an Australian law, that is of the same nature as, or a substantially similar nature to the foreign offence.

4.19 Several submitters expressed concern that, in context of an investigation for a foreign offence,

- what constitutes a serious offence in the requesting country may not be treated as a criminal offence at all in Australia; and
- that conduct may be categorised differently and treated as more or less seriously in the foreign country and be out of step with Australian values.[14]

4.20 The NSW Office of the Privacy Commissioner argued that the personal information about Australian citizens should not be made available to foreign countries for the purpose of prosecuting individuals for conduct which would not constitute an offence in Australia.[15] These concerns were shared by several groups, including the Australian Privacy Foundation and NSW Council of Civil Liberties.[16] Electronic Frontiers Australia argued for clearer safeguards to ensure that foreign countries would not have access to stored communication to investigate dissident activity in repressive states.[17] Similarly, the Australian Privacy Foundation cautioned against creating any obligation to foreign countries that might have a chilling effect on freedom of political speech of anyone resident in Australia.[18]

4.21 The Law Council of Australia also argued that foreign penalties may be more severe than the penalties imposed in Australian jurisdictions for like conduct.[19] Several participants argued that, under no circumstances,

13 *Explanatory Memorandum*, p. 21.

14 For example, Law Council of Australia, *Submission 5;* Australian Privacy Foundation, *Submission 16*.

15 New South Wales Office of the Privacy Commissioner, *Submission 22*, p. 3.

16 New South Wales Council for Civil Liberties, *Submission 21*.

17 Electronic Frontiers Australia, *Submission 8*, p. 3.

18 Australian Privacy Foundation, *Submission 16*, p. 12.

19 Law Council of Australia, *Submission 5*, p. 5.

should Australia be providing assistance where there was a possibility of the imposition of the death penalty.[20]

4.22 The treatment of breaches of copyright was raised as a specific example where Australia may differ from other jurisdictions. Infringement of copyright is a criminal offence in some jurisdictions but is generally treated as a civil matter in Australia, with indictable offences only available for large commercial scale infringements.[21]

4.23 Conversely, Australia may categorise some conduct as a serious criminal offence and impose a higher penalty than comparable European countries. The Uniting Church of Australia's advised that the research of the International Centre for Missing and Exploited Children, illustrated the lack of comparative penalties. Many countries, including many European countries, impose a maximum penalty of two years imprisonment for the possession, dissemination, sale or rent of child sexual abuse material.[22]

4.24 Accordingly, the United Church fears that stored communications warrants will not be available to investigate a significant amount of online child sexual exploitation and related offences.[23] To overcome this perceived deficiency, the Uniting Church argued for specific reference in proposed section 15B to make stored communications warrants available for the investigation of foreign offences relating to child sexual abuse and child grooming online.[24]

4.25 An alternative approach was suggested by the Australian Privacy Foundation. The Foundation suggested that, to remove doubt, the proposed section 5EA of the TIA Act be amended to define a serious foreign contravention as a contravention that is punishable by the requisite maximum penalty and where the conduct is subject to an equivalent or substantially similar Australian law.[25]

---

20 Queensland Council of Civil Liberties, *Submission 12,* p. 3; NSW Council of Civil Liberties, *Submission 21.*

21 The *Copyright Act 1968* provides a broad range of criminal offences. Part V, Division 5 of the Copyright Act contains both indictable, summary and, (in some instances) strict liability offences in relation to certain commercial scale infringing activities and various acts to do with infringing copies, including making them commercially, selling, hiring, offering for sale, exhibiting in public, importing commercially, distributing and possessing for commence. As the Copyright Act already contains extensive criminal offences, accession to the Convention does not require Australia to enable any additional offences.

22 Uniting Church in Australia, Synod of Victoria and Tasmania, *Submission 13*, p. 7.

23 Uniting Church in Australia, Synod of Victoria and Tasmania, *Submission 13*, pp. 6-7.

24 Uniting Church in Australia, Synod of Victoria and Tasmania, *Submission 13*, p. 7.

25 Australian Privacy Foundation, *Submission 16*, p. 12.

Conditions of disclosure

4.26 The Law Council of Australia supported the proposed section 142A of the TIA Act, but queried how, in the absence of an undertaking, these conditions would be communicated, imposed, accepted and enforced. Similarly, Mr Bruce Arnold, an academic lawyer specialising in telecommunication law, said that Australian authorities are bound under the TIA Act not to misuse the information, but have no control of what foreign agencies see the information and what those agencies do with the information.[26]

4.27 The Committee sought advice from Telstra on whether it had any views about the potential for secondary uses of its customer's information. In reply Telstra advised that:

> Telstra is always concerned about the possible secondary uses of its customers information once that information has been lawfully provided to third parties. However, it considers that it is for the Government to establish the appropriate protections (such as legislative prohibitions) to ensure secondary uses is in line with government policy.[27]

4.28 To address this uncertainty, the Law Council of Australia suggested that subsection 8(2) of the MA Act be amended to include an additional discretionary ground for refusing a mutual assistance request, that would encourage the Attorney-General to decline a request where the requesting country's arrangements for handling personal information do not offer privacy protection substantially similar to those applying in Australia.[28]

4.29 The mutual assistance regime is discussed below.

Mutual assistance regime

4.30 In response to some of the concerns, the Attorney-General's Department gave evidence to the Committee that all the existing safeguards of the current MA Act will continue to apply.[29] For example, the Attorney-General must decline a request where the offence is a political offence, the person has already been acquitted or pardoned (double jeopardy) or

26 Mr B Arnold and Ms Masters, *Submission 18,* p. 3.

27 Telstra Corporation Limited, *Supplementary Submission 14*.1, p.1.

28 Law Council of Australia, *Submission 5,* p. 7.

29 Mr Andrew Kiley, Senior Legal Officer, International Crime Cooperation Division, Attorney-General's Department, *Committee Hansard*, 1 August 2011, p. 29.

because providing assistance would prejudice the sovereignty, security or national interest of Australia (paragraphs 8(1) (a)–(f) of the MA Act).

4.31 Assistance may also be refused on a number of other grounds, including,:

- where the conduct is not an offence in Australia;
- where if it occurred in Australia the offence could not be prosecuted because of lapse of time or other reasons;
- would prejudice an Australian investigation; or
- would impose an excessive burden on Commonwealth, state or territory resources (subsection 8(2) of the MA Act).

4.32 The consideration of dual criminality in paragraph 8(2) (a) of the MA Act does not require the penalty associated with the offence in both countries to be substantially similar. The issue of the comparative levels of penalty for conduct that is criminal in both jurisdictions may be considered by the Minister through the general discretion not to provide assistance where appropriate in all the circumstances of the case (paragraph 8(2) (g) of the MA Act).

Committee View

4.33 The European Convention requires States parties to provide investigative tools that are available to its domestic law enforcement agencies to their foreign counterparts. The Convention, however, does not require that any domestic conditions, standards or safeguards need be lowered to accommodate mutual assistance. As a matter of principle, the same threshold should apply to a foreign country as applies to domestic law enforcement agencies.

4.34 As has been noted above, the seriousness with which crimes (or not) are treated in Australia and foreign countries has attracted significant comment by participants in the inquiry.

4.35 The Committee sees merit in the argument by the Australian Privacy Foundation that a dual criminality test be added to the threshold for accession to requests by foreign countries for stored communications warrants. However, the Committee does not see how this issue can be fully resolved by amendment to this Bill without also disturbing the mutual assistance framework more generally. Further, some of the specific

concerns raised in evidence, for example, in relation to political offences, are dealt with already in the MA Act.

4.36 However, the possibility that Australia may not provide assistance in relation to some child sexual exploitation offences is a matter of concern as the Committee and the Australian community treat such offenses very seriously. Consequently, there may be an argument to approach such offences, which are mandated by Article 9 of the Convention, differently to other offences.

Recommendation 1

That the thresholds that apply to the issuing of a stored communication warrant under the *Mutual Assistance in Criminal Matters Act 1987* and the *Telecommunications (Interception and Access) Act 1979* for an investigation or investigative proceeding for a serious foreign offence be the same thresholds as apply for domestic Australian investigations.

Recommendation 2

That the Attorney-General investigate whether the proposed new Part IIIA of the *Mutual Assistance in Criminal Matters Act 1987* may prevent stored communications warrants being available to foreign countries for investigations into child sexual exploitation.

Recommendation 3

That subsection 8(2) of the *Mutual Assistance in Criminal Matters Act 1987* be amended to include an additional discretionary ground to decline a request where the requesting country's arrangements for handling personal information do not offer privacy protection substantially similar to those applying in Australia.

Disclosure of Prospective Telecommunications Data

4.37 The Bill proposes to amend the MA Act and the TIA Act to enable the Attorney-General to authorise the AFP to disclose telecommunications data, collected on an ongoing basis, for an investigation into a foreign criminal offence.

Threshold

4.38 Under proposed section 15D of the MA Act, the Attorney-General must have:

- received a request for mutual assistance for a foreign country; and
- be satisfied an investigation has commenced into a serious foreign criminal offence.

4.39 The section will apply if a foreign country requests disclosure of specific information or documents that come into existence during a specified period (i.e. into the future).[30]

Safeguard

4.40 The Bill also proposes to amend the TIA Act, by inserting new section 180B to provide that an authorised officer of the AFP may disclose prospective telecommunications data if the officer is satisfied the disclosure is:

- reasonably necessary for the investigation of an foreign offence (punishable by imprisonment for three or more years, life or the death penalty); and
- appropriate in all the circumstances.[31]

4.41 As the disclosure may only occur once the Attorney-General has agreed to grant mutual assistance, the disclosure of the prospective data may be subject to conditions set by the Attorney-General.

---

30 The Explanatory Memorandum to the Bill states that the definition of prospective telecommunications data means the fact that specified information or a document has passed over the system, but does not include the content.

31 Proposed subsection 180B(8) of the TIA Act.

4.42 Proposed section 180B of the TIA Act will provide that an authorisation may be given for a maximum of 21 days and may be extended once only, for a further 21 days.

Conditions of disclosure

4.43 The information may not be disclosed unless it is subject to conditions set out in proposed new section 180E of the TIA Act. These conditions include that:

- the information will only be used for purposes for which the information was requested;
- that the document or other thing containing the information will be destroyed when it is no longer required for those purposes; and
- in the case of a disclosure under section 180B, any other condition determined, in writing, by the Attorney-General.

General Privacy Safeguard

4.44 The Bill also proposes to insert section 180F to the TIA Act as a general privacy safeguard applicable to disclosures to foreign countries and in the context of domestic investigation. It will apply to all forms of disclosure of historic, prospective telecommunications data. Proposed new section 180F replaces existing section 180(5) of the TIA Act and is essentially the same formula. The proposed section states that before making a disclosure the authorising officer:

> must have regard to how much the privacy of any person or persons would be likely to be interfered with by the disclosure or use.[32]

Commentary

4.45 Some critics of the Bill argued that the requirement that an officer only disclose information where it is 'appropriate in all the circumstances' is an inadequate safeguard.[33] The Explanatory Memorandum to the Bill states that this is intended to allow the AFP to consider 'other relevant factors'

32 Proposed section 180F of the TIA Act.

33 For example, Law Council of Australia, Submission 5; Australian Privacy Foundation, Submission 16.

but does not illustrate what those factors might be.[34] Nor does the proposed section 180B provide any direction on what weight is to be given to these factors, or how the question of proportionality is to be decided.

4.46 Further, proposed section 180F of the TIA Act will only require the AFP to 'have regard to how much the privacy of any person or persons would be likely to be interfered with by the disclosure'.[35] The Law Council of Australia questioned the value of a legislative provision which merely requires an authorising officer to 'have regard' to privacy impacts.[36]

4.47 Similarly, the Australian Privacy Foundation said that while a privacy test would be welcome, the proposed section does not amount to a meaningful test.[37] It was argued that:

> This is not in any sense a protection, because it fails to impose and obligation to form a judgment as to whether the extent of the interference is justified, and hence it is open to the authorising officer to proceed unfettered.[38]

4.48 The intent of proposed section 180F is set out in the Explanatory Memorandum, which states that the intent is for:

> ...wider considerations to be made prior to making an authorisation, including the amount of information that making the authorisation will give the agency, the relevance of the access information to the investigation in question, as well as how third parties' privacy may be impacted by accessing this information.[39]

4.49 Both the Law Council of Australia and the Australian Privacy Foundation suggested that the statutory language of the Bill should elaborate a test that more accurately reflects the intention, as expressed in the Explanatory Memorandum.[40]

34 *Explanatory Memorandum*, p. 40.
35 *Explanatory Memorandum*, p. 40.
36 Law Council of Australia, *Submission 5*, p. 10.
37 Australian Privacy Foundation, *Submission 16*, p. 9.
38 Australian Privacy Foundation, *Submission 16*, p. 9.
39 *Explanatory Memorandum*, p. 43; Law Council of Australia, *Submission 5*, p. 11.
40 Law Council of Australia, *Submission 5*, p.11; Australian Privacy Foundation, *Submission 16*, p. 9.

Committee View

4.50 The Committee accepts that the thresholds and safeguards applied to police disclosures of prospective telecommunications data reflect the less intrusive nature of non-content data. However, the general privacy test in proposed section 180F of the TIA Act was singled out by inquiry participants as ineffective in its current form. The Explanatory Memorandum already provides guidance on the interpretation of the provision. It, therefore, seems possible to amend the proposed section 180F to better reflect the intention of the Bill without imposing any further burden on the AFP. This approach will provide greater visibility and public confidence in the legislation.

Recommendation 4

That proposed section 180F of the *Telecommunications (Interception and Access) Act 1979* is amended to elaborate more precisely the requirement that the authorising officer consider and weigh the proportionality of the intrusion into privacy against the value of the potential evidence and needs of the investigation.

5

Police Assistance to Foreign Countries – Historic and Existing Telecommunications Data

Introduction

5.1 This chapter discusses aspects of the Cybercrime Legislation Amendment Bill 2011 (the Bill) intended to allow:

- disclosure and sharing of 'historical telecommunications data' with foreign law enforcement authorities without the need for a formal request for mutual assistance on a police-to-police basis; and
- sharing of 'existing telecommunications data', namely, data already disclosed for domestic law enforcement purpose (a secondary disclosure) with foreign law enforcement authorities without the need for a formal request for mutual assistance on a police-to-police basis.

5.2 The disclosure and sharing of prospective telecommunications data under a mutual assistance request is dealt with in Chapter Four.

Background

5.3 Under the *Telecommunications (Interception and Access) Act 1979* (TIA Act), direct access to historical telecommunications data by police, without the need for a warrant, is regulated under an authorisation mechanism set out in Chapter 4 of the TIA Act.

5.4 Telecommunication data is not defined in the TIA Act but is generally equivalent to the concept of 'traffic data', which is extensively defined in the Council of Europe Convention on Cybercrime.[1] In Australian law, telecommunications data is any data other than the substance or content of a communication.[2] It includes, for example, subscriber details and call charge records.

5.5 Under the TIA Act, enforcement agencies have discretion to authorise the disclosure of non-content information in existence at the time an authorisation is made (historical telecommunications data).[3] The authorising officer must be satisfied that the disclosure is reasonably necessary for the enforcement of the criminal law, a law imposing a pecuniary penalty or for the protection of the public revenue.[4]

5.6 Historical telecommunications data may be disclosed to a foreign country for the investigation or prosecution of foreign criminal offences through the use of a search warrant under existing section 38C of the *Mutual Assistance in Criminal Matters Act 1987* (MA Act). The Attorney-General's Department argued that the existing mechanism 'can be time consuming'.[5]

5.7 Under the TIA, prospective telecommunications may not be passed to a foreign country. The Bill proposes to allow for disclosure of ongoing telecommunications data to foreign country, once a formal mutual assistance request has been approved by the Attorney-General. This aspect of the Bill is dealt with elsewhere in this report.

Cybercrime Legislation Amendment Bill 2011

Primary disclosure of historical telecommunications data

5.8 The Bill proposes to remove the current oversight requirements for disclosure of historic telecommunications data, namely, a mutual assistance request approved by the Attorney-General and a search warrant be granted by an independent issuing authority.

1 Article 1(b) of the Council of Europe Convention on Cybercrime.

2 The term 'telecommunications data' is not defined in the *Telecommunications (Interception and Access) Act 1979* (TIA Act). However, section 172 of the TIA Act prohibits the disclosure of the content or substance of the communication when disclosing information or a document under this part of the Act

3 Section 178 of the TIA Act.

4 Subsections178 (1) (2) (3), and 179 (1)(2)(3) of the TIA Act.

5 *Explanatory Memorandum*, Cybercrime Legislation Amendment Bill 2011, p. 36.

5.9 Proposed section 180A will provide the basis for the Australian Federal Police (AFP) to authorise the disclosure of specified historical telecommunications data (i.e. in existence prior to the notification) to a foreign country for the purposes of the enforcement of foreign criminal law.[6] The authority to order such disclosures will be limited to the Commissioner, Deputy Commissioner or senior executive of the AFP.[7]

5.10 The initial threshold test, (satisfaction that the disclosure is reasonably necessary for the enforcement of foreign criminal law) is the same as for a domestic purpose.

5.11 The threshold for disclosure to a foreign law enforcement agency will be that the officer must not be authorised unless the officer is satisfied that:

- the disclosure is reasonably necessary for the enforcement of the criminal law of a foreign country; and
- the disclosure is appropriate in all the circumstances.[8]

5.12 A foreign law enforcement agency will be defined as a police force of a foreign country or any other authority or person responsible for law enforcement of that country.[9]

Secondary disclosure of existing telecommunications data

5.13 Existing sections 178 and 179 of the TIA Act enable an authorised officer to authorise the disclosure of existing information or documents for the purpose of enforcing domestic criminal law, a law that imposes a pecuniary penalty or for protecting the public revenue.

5.14 The Bill proposes to insert new section 180C, to enable passage of telecommunications data already disclosed for domestic law enforcement purpose to a foreign law enforcement agency. The sharing of existing data will be limited to criminal law purposes.[10] Data relating to locating a missing person is also excluded.

5.15 The threshold will be the same as that which applies to disclosure of historical telecommunications data for a foreign law enforcement purpose. Namely, the authorised officer must be satisfied that the disclosure is:

---

6 *Explanatory Memorandum*, p. 36.

7 Proposed subsection 5A (1A) of the TIA Act.

8 Proposed subsection 180A (5) of the TIA Act.

9 Amendment to subsection 5(1) of the TIA Act.

10 Proposed subsection 180C (2) of the TIA Act.

- reasonably necessary for the enforcement of the criminal law of a foreign country; and
- appropriate in all the circumstances.[11]

Privacy safeguard

5.16 The general privacy test contained in proposed section 180F, mentioned earlier, also applies to disclosures of telecommunications data to a foreign country.[12]

Restriction on use, disclosure, retention and destruction of telecommunications data

5.17 Proposed section 180E provides that telecommunications data may not be disclosed to a foreign country unless the disclosure is subject to the following conditions:

- that the information will only be used for the purposes for which it is requested; and
- that any document or other thing containing the information will be destroyed when it is no longer required for those purposes.[13]

5.18 In the context of prospective telecommunications data, disclosure under a mutual assistance request, the Attorney-General may impose conditions on the use, disclosure, retention and destruction of the information.

Commentary

Thresholds

5.19 The Law Council of Australia argued, while it does not object to police to police assistance in principle, the ability of Australian law enforcement agencies to share such data directly with counterparts overseas should be subject to strict conditions. The Law Council of Australia said:

> While telecommunications data does not include the content and substance of a person's private communications, it nonetheless

11 Proposed 180C (2) of the TIA Act.

12 See Law Council of Australia, *Submission 5*; Privacy Foundation of Australia, *Submission 16*.

13 Proposed subparagraphs180E (1) (a) (b) (c) of the TIA Act.

> may reveal information about crucial and private matters such as a person's associations and movements. Therefore strict conditions should attach to the disclosure and use of such information.[14]

5.20 The threshold that the disclosure is 'appropriate in all the circumstances' was considered too ambiguous to act as an effective safeguard. Further, the Bill does not provide guidance to the relevant officer about the types of matters the legislature intends that he or she should consider before authorising disclosure.[15] The Explanatory Memorandum simply states that the Bill is:

> ...intended to allow the authorised officer to consider other relevant factors in determining whether it is appropriate to make the disclosure.[16]

5.21 Other submitters pointed out that removal of the Attorney-General's scrutiny, would also mean there will be no requirement for consideration of whether the offence,

- is a political offence;
- potentially attracts the death penalty;
- involves double jeopardy;
- lacks dual criminality; or
- is a military offence.

5.22 For example, Mr Phillip Hall said:

> Australia should not provide information to a foreign country in relation to an offence for which the death penalty could be imposed. Public debate around the Australian Federal Police's cooperation with Indonesian authorities in relation to the "Bali 9" highlighted this issue.[17]

5.23 These are all grounds for refusing a mutual assistance request. Removal of the Attorney-General's scrutiny also removes an opportunity to subject the disclosure to conditions that reflect Australian values.

5.24 The European Convention expressly provides that traffic data may be withheld if the request concerns a 'political offence' or is likely to

14 Law Council of Australia, *Submission 5,* p. 8.
15 Law Council of Australia, *Submission 5,* p. 8.
16 Law Council of Australia, *Submission 5,* p. 8.
17 Mr Phillip Hall, *Submission 19*, p. 1.

'prejudice its sovereignty, security, *ordre public* or other essential interests' (Article 30(2)). Additionally, while States parties are required to make available the same investigative as exist for domestic investigations, the Convention explicitly requires that powers and procedures to be subject to the conditions, standards and oversight applicable in the country.[18]

5.25 The Law Council of Australia proposed that this perceived deficiency could be overcome by, at the least, amending the Bill to provide that:

> Without limiting sub-section 180(5)(b) and 180C(2), in determining whether a disclosure is appropriate in all the circumstances, the authorising officer must give consideration to the mandatory and discretionary grounds for refusing a mutual assistance request as limited in section 8 of the Mutual Assistance [in Criminal Matters] Act.[19]

5.26 Mr Hall argued that cooperation in relation to offences that carry the death penalty should be excluded from the Bill entirely.[20] If the Government persist in creating a power to share telecommunications data in these circumstances, it should be considered so serious that it should only happen in exceptional circumstances, and should require the consent of the Attorney-General.[21]

Dual criminality

5.27 The concerns about the alignment of Australian and foreign offences were expressed in relation to police to police assistance for historical and existing data. It was argued, that while the provisions restrict these types of disclosure to a foreign criminal offence, attracting at least a maximum penalty of three years, the lack of dual criminality may result in the sharing of information for investigations that are incompatible with Australian values. The issues associated with dual criminality are discussed in Chapter Four.

Privacy safeguard

5.28 Issues relating to proposed section 180F are discussed in chapter four about access to stored communications under the mutual assistance

18 Article 15 specifically requires States to subject procedural powers to safeguards to protect human rights. This includes judicial or other independent supervision, grounds justifying an application, and limitation of the scope and the duration of the power or procedure.

19 Law Council of Australia, *Submission 5,* p. 8.

20 Mr Phillip Hall, *Submission 19*, p. 1.

21 Mr Phillip Hall, *Submission 19*, p. 1.

regime. Proposed section 180F also applies in the context of police disclosure of telecommunications data to a foreign country.

5.29 The Law Council of Australia again submitted that the proposed section be expressed in terms of a clear test directing the authorising officer to be satisfied that the likely benefit of the disclosure substantially outweighs the extent to which the disclosure interferes with the privacy of any person(s).[22] This would align the statutory formula with the intention expressed in the Explanatory Memorandum.

Conditions of disclosure

5.30 As mentioned above, the proposed new section 180E of the TIA Act provides that telecommunications data may not be disclosed to a foreign country unless there is an assurance that the information will only be used for the purposes for which it requested and that the data will be destroyed when it is no longer required. The adequacy of these conditions for disclosure was questioned by the Australian Privacy Foundation, which stated:

> Any information disclosed from Australia to a foreign country must have specific restrictions that prohibit secondary use of disclosed information. It should be irrelevant whether the information disclosure is conducted through an agency transfer or one governed by restrictions made by the Attorney-General.[23]

5.31 The concern about lack of restriction on secondary use was compounded by the unrestricted nature of the 'foreign countries' to which sensitive personal data could be shared.[24] The Australian Privacy Foundation believed strongly that the disclosure of telecommunication data should be restricted to States that are parties to the Convention.[25]

5.32 It was argued that the Bill should impose strict limitations on the purposes for which data may be preserved, collected, used and disclosed; expressly prohibit secondary uses of all telecommunications data (prospective, historic and existing); and ensure the limitations are imposed on any other person that may come into possession of the data.[26]

---

22 Law Council of Australia, *Submission 5*, p. 8.
23 Privacy Foundation of Australia, *Submission 16*, p. 10.
24 Privacy Foundation of Australia, *Submission 16*, p. 10.
25 Privacy Foundation of Australia, *Submission 16*, p. 10.
26 Privacy Foundation of Australia, *Submission 16*, p. 10.

5.33 As previously mentioned, in Chapter 4, the Committee sought advice from Telstra on any concerns it may have about secondary use of its customer's information. Telstra said that it did have concerns, and that it was a matter for Government to apply legislative prohibitions to ensure secondary use is in line with government policy.[27]

5.34 The Attorney-General's Department, and the AFP submitted that international cooperation works on the basis of reciprocity and they were unaware of any inappropriate use of information shared by Australia with overseas agencies.[28] The AFP told the Committee that the AFP shares information with international counterparts through mutual assistance arrangement on a daily basis and the same principle of reciprocity applies in the police-to-police context.[29] The AFP also said:

> As much as we can be confident that another law enforcement agency will treat our information in accordance with our own laws we are but I do not think, from a police perspective, that I can give a 100 per cent guarantee that that is going to be the case. Rest assured that, if they breach our trust, the relationship will sour to the extent that we will not be assisting in the future.[30]

Notification to data subjects

5.35 Neither the Bill nor the principal TIA Act make any requirement for law enforcement agencies to notify a person who is subject to an intercept warrant, stored communication warrant, or disclosure authorised under Chapter 4. In evidence to the Committee, it was argued that once notification of a subject would no longer prejudice any investigation that, that person(s) who were the subject of the interception, access or disclosure should be notified.[31]

5.36 The Committee sought further advice, and was informed that under wiretap laws in the United States of America, subjects of an interception warrant are notified of that fact once there is no prejudice to an

27 Telstra, *Supplementary Submission 14.1*, p.1.

28 Mr Andrew Kiley, Senior Legal Officer, International Crime Cooperation Division, Attorney-General's Department, *Committee Hansard*, Canberra, 1 August 2011, p. 30.

29 Assistant Commissioner Gaughan , National Manager, High Tech Crimes Operations, Australian Federal Police, *Committee Hansard*, Canberra, 1 August 2011, p. 30.

30 Assistant Commissioner Gaughan, Australian Federal Police, *Committee Hansard*, Canberra, 1 August 2011, p. 30.

31 Privacy Foundation of Australia, *Submission 16*, p. 10.

investigation. This was confirmed by the Attorney-General's Department.[32]

5.37 At the request of the Committee, and in the short time available, the Australian Privacy Foundation sought advice from an expert in Europe on this matter. The Foundation was advised that in the United Kingdom the *Regulation of Investigatory Powers Act* (RIPA) does not require subjects to be notified. However, the accompanying Code of Practice issued by the British Home Office notes that there is no provision of the RIPA that prevents a carriage service provider from informing a person in response to a request from the subject.[33]

5.38 Additional advice from Germany, was that:

> Under German Criminal Procedure Law there is an obligation to notify data subjects when their communications have been intercepted as soon as an ongoing criminal investigation would not be prejudiced by such notice. This seems to be congruent with your submission. The same applies to wiretapping by secret services. However, [freedom of information (FOI)] laws would not apply in this area since the Criminal Procedure Act or federal laws governing the secret service would pre-empt application of FOI laws.[34]

Committee View

Threshold

5.39 The ability to take the initiative to share telecommunications data with a foreign country will enhance the ability of the AFP to work proactively with foreign counterparts. The authorisations mechanism already reflects the distinction between content and traffic data and provides for expeditious use of this less intrusive method.

---

32 Ms Catherine Smith, Assistant Secretary, Telecommunications Surveillance Law Branch, Attorney-General's Department, *Committee Hansard*, Canberra, 1 August 2011, p. 32.

33 Australian Privacy Foundation, *Supplementary Submission 16.1*, p. 1. The advise notes that an exemption to access may be exercised by the carrier under the United Kingdom's *Data Protection Act*. This decision would be open to review.

34 Correspondence, Australian Privacy Foundation of Australia, 9 August 2011.

5.40 However, there are justified concerns about the unrestricted sharing of telecommunications data with foreign countries. As previously noted, foreign countries in this context are not limited to States parties to the European Convention or to those countries which whom Australia already has a formal mutual assistance arrangement. The ability to share is 'at large'.

5.41 In these circumstances, the Committee believes the public will have more confidence in the new regime if there is meaningful guidance to police. The alignment of the TIA Act with the MA Act would provide clarity to the police on factors to be considered; visibility to the public and also be consistent with the European Convention.

Recommendation 5

That proposed sections 180A (5) and 180C (2) of the *Telecommunications (Interception and Access) Act 1979* be amended to ensure that, in determining whether a disclosure of telecommunications data to a foreign country is appropriate in all the circumstances, the authorising officer must give consideration to the mandatory and discretionary grounds for refusing a mutual assistance request under existing section 8 of the *Mutual Assistance in Criminal Matters Act 1987*.

Recommendation 6

That the disclosure of telecommunications data to a foreign country in the context of police to police assistance at the investigative stage and in relation to criminal conduct that, if prosecuted, may attract the death penalty, must:

(a) only take place in exceptional circumstances and with the consent of the Attorney-General and the Minister for Home Affairs and Justice; and

(b) each Minister must ensure that such consent is recorded in a register for that purpose.

5.42 The Committee's views and recommendations concerning dual criminality, and the generic privacy test are set out in Chapter Four and apply equally in the context of police to police assistance.

5.43 The Committee shares some of the uncertainty about potential misuse of information shared with foreign countries. However, reciprocity is the guiding principle of police-to-police cooperation and trust and the committee appreciates the assurance given by the AFP.

5.44 Nevertheless, it is widely accepted that the European Convention operates within the wider framework of European law, at the European Union and national levels. Privacy law is highly developed, and governs the transfer and protection of transborder information flows between agencies. Privacy is matter of high public importance, and while Australian privacy law and practice is also highly developed it does not operate in conjunction with the wider European system. It may therefore be useful to clarify the conditions of disclosure to avoid any unintended vagueness as to Australia's intentions in this regard. This seems a reasonable compromise to the Committee if the Bill is to retain an unrestricted definition of foreign country, and not be limited to States parties to the European Convention.

Recommendation 7

That the Cybercrime Legislation Amendment Bill 2011 be amended to elaborate the conditions of disclosure of historical and existing telecommunications data to foreign countries, including in relation to retention and destruction of the information and an express prohibition on any secondary use by the foreign country.

5.45 The Committee also considers there is merit in investigating the potential for notifying data subjects about a previous interception, preservation, access or disclosure once the disclosure could be done without risking prejudice to an ongoing investigation.

Recommendation 8

That the Attorney-General investigate the desirability and practicality of a legislative requirement for data subjects to be advised that their communications have been subject to an intercept, stored communications warrant, or telecommunications data disclosure under the *Telecommunications (Interception and Access) Act 1979* once that advice could be given without prejudice to an investigation.

6

Commonwealth Computer Offences

Introduction

6.1 As noted in Chapter One, the Council of Europe Convention on Cybercrime (European Convention) requires States parties to establish a range of computer offences including:

- access to a computer system without right (Art 2);
- interference with data without right (Art 4);
- interference with the functioning of a computer system without right (Art 5); and
- the production, sale, procurement for use, import distribution a device or access data with intent of committing a computer offence (Art 6).

6.2 In addition to specific computer offences, Articles 7 to 11 require States parties to criminalise computer related offences such as forgery, fraud, child pornography, copyright infringements and related ancillary conduct. These obligations are already implemented in Australia through a mix of Commonwealth and State and Territory law.

6.3 The Constitution does not grant the Commonwealth express legislative power over criminal activity *per se*. However, the Commonwealth Parliament can validly make laws to create criminal offences and provide for their investigation, prosecution and punishment, provided that the offences fall within, or are incidental to the exercise of a constitutional head of power.

6.4 Existing Commonwealth computer offences are provided for in Part 10.7 of the *Criminal Code Act 1995*. Part 10.7 computer offences cover acts of

illegal access, modification and impairment of computer data and are limited to conduct that involves a Commonwealth computer or computer systems, Commonwealth data or commission of crimes by means of a telecommunications service.

6.5 The offences were based on model laws developed by the Model Criminal Code Officers Committee in 2001 and have not been uniformly implemented across all Australian jurisdictions. However, State and Territory computer offences apply generally in their respective jurisdictions and therefore provide national coverage in practice.

Cybercrime Legislation Amendment Bill 2011

6.6 Schedule 3 of the Cybercrime Legislation Amendment Bill 2011 (the Bill) repeals the current restrictions that apply to the Commonwealth offences, removing any requirement that the offence relate to commonwealth property or be conduct via a telecommunications service.[1] The effect of these amendments is to use the Commonwealth's external affairs power under the Constitution to create comprehensive computer offences which are compatible with articles two, four and five of the European Convention.

6.7 None of the States or Territories objected to Australia acceding to the European Convention on Cybercrime. However, some States expressed concern about the impact of unrestricted national offences on the validity of concurrent to State law

6.8 The Commonwealth Attorney-General's Department has said that, by removing the constitutional limits on the computer offences, Australia will overcome the patchy coverage of computer crime across the various Australian jurisdictions.[2] The Committee was told that the existing savings provisions of the Criminal Code will apply, so that in the event of *any inconsistency* with State and Territory laws, State and Territory law will still be valid.[3] In other words, although the proposed Commonwealth computer offences would operate without restriction, it is not the intention of the Commonwealth to 'cover the field'. Finally, the Explanatory Memorandum to the Bill also states that:

1 *Explanatory Memorandum*, Cybercrime Legislation Amendment Bill 2011, p. 47.

2 Ms Catherine Smith, Assistant Secretary, Telecommunications Surveillance Law Branch, Attorney-General's Department, *Committee Hansard*, Canberra, 1 August 2011, p. 24.

3 Ms Catherine Smith, Attorney-General's Department, *Committee Hansard*, Canberra, 1 August 2011, p. 24.

> Ensuring that Commonwealth laws meet the obligations under articles 2,4 and 5 of the Convention, without reliance on State and Territory laws, will also ensure that the jurisdictional obligations of article 22 of the Convention are fulfilled in respect of those offences.[4]

6.9 Article 22 of the European Convention requires States parties to extend jurisdiction to offences:

- in its territory;
- on board a ship flying the flag of that Party;
- on board an aircraft registered under the law of that Party; or
- by one of its nationals, if the offence is punishable under the criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.

6.10 In its National Interest Analysis for accession to the European Convention, the Commonwealth indicated that Australia proposes to make a reservation in relation to Article 22(2) of the Convention and comply with the Convention through a combination of Commonwealth and State laws.[5] The Committee understands that this is because State and Territory laws do not meet the jurisdictional obligations of Article 22 of the Convention.[6]

Impact on the validity of concurrent State criminal offences

6.11 The governments of Western Australia, Victoria and New South Wales told the Committee that they support Australia's accession to the Convention provided that accession does not lead to conflicts between Commonwealth, State and Territory offence provisions.[7]

6.12 The Committee's attention was drawn to the current uncertainty over the constitutional division of legislative power to make laws with respect crime. On 22 September 2010, the High Court handed down its judgment in *Dickson v The Queen* [2010] HCA 30, in which the Court invalidated certain Victorian legislative provisions (conspiracy to steal

4 *Explanatory Memorandum*, p. 47.

5 *National Interest Analysis* [2011] ATNIA 9, Accession by Australia to the Convention on Cybercrime, paragraph 36. See also Premier of Western Australia, *Submission 11*, p. 3.

6 Article 22(2) permits States parties to make a reservation in relation to extended jurisdiction, ie where an offences is committed outside the territorial borders of the state or by a national outside the territorial borders of any state.

7 Premier of Western Australia, *Submission 11*; Robert Clark MP, Victorian Attorney-General, *Submission 17*; New South Wales (NSW) Government, *Submission 23*.

Commonwealth property).[8] The decision has brought into question the approach to resolving questions of the validity of concurrent and overlapping State and Commonwealth offences more generally.

6.13 The Victorian Attorney-General, Mr Robert Clark MP, has advised that in the *Dickson Case* the High Court took a broader view of what counts as constitutional inconsistency than many previously expected and this has introduced a notable degree of uncertainty into the constitutional law governing overlapping criminal laws.[9]

6.14 Similarly, Associate Professor Dr Jeremy Gans of the University of Melbourne submitted that, in his opinion, the judgment appears to stand for the proposition that a state criminal law will be invalid to the extent of its overlap with federal criminal law, if the federal criminal law includes protections for defendants not available under state law.[10] He concluded that, as the Bill will widen the area of overlap between federal and stated offences, the potential scope for invalidity will be extended to include computer offences.[11] Dr Gans also observed that, if passed, the potential for invalidity would:

> ... include computer offences that involve neither federal crimes, federal computers nor the internet.[12]

6.15 In the case of Victoria, it was explained that the proposal to remove the nexus with the Commonwealth from the existing offences so that:

> Such an expansion of the scope of federal criminal offences in this area would mean that there would be a significant degree of overlap between the Commonwealth's computer offences and Victoria's existing computer offences in ss. 247A to 247I of the *Crimes Act 1958 (*Vic).[13]

6.16 The Government of Western Australia has also raised concerns about the impact of broader Commonwealth offences, rather than Australia's traditional reliance on a combination of Commonwealth and State and Territory criminal laws.[14] The Premier of Western Australia informed the committee that the Bill would potentially render invalid offence

---

8 (2010) 241 CLR 491.

9 Victorian Attorney-General, *Submission 17*, p. 2.

10 Dr Jeremy Gans, *Submission 2*, p. 3.

11 Dr Jeremy Gans, *Submission 2*, p. 2.

12 Dr Jeremy Gans, *Submission 2*, p. 2.

13 Victorian Attorney-General, *Submission 17*, p. 1.

14 Premier of Western Australia, *Submission 11*, p. 1.

provisions that are stronger, more far reaching and comprehensive than the Commonwealth offences.[15]

Direct versus indirect inconsistency

6.17 The Commonwealth Attorney-General's Department has assured the Parliament that, in the event of 'any inconsistency the savings provisions of the Criminal Code, will protect the validity of State laws.[16] However, the Committee notes that the state governments of NSW, Victoria and WA as well as Dr Gans have all made submissions that differ from this view.

6.18 Participants in the inquiry argued that the savings provisions of the Commonwealth Code do not have the effect of protecting the validity of State law when the inconsistency is *direct* (as opposed to indirect).[17] In other words, where the offences are in fact concurrent and overlapping the likelihood of invalidity is increased despite the savings provision. The NSW government advised, for example, that NSW has implemented the model code computer offences. Removing the 'carriage service' and 'Commonwealth computer' limitation from Part 10.7 would effectively create identical offences under NSW and Commonwealth legislation.[18]

6.19 Moreover, in the *Dickson Case*, the High Court reached its conclusion that part of Victoria's criminal law was invalidated by the Commonwealth Code despite the presence of a savings clause for state criminal offences in the theft provisions of the *Criminal Code 1995* (Cth).[19]

6.20 Further, expert evidence is that invalidation of a State law cannot be remedied by retrospective State legislation, as a result of an earlier High Court decision in 1984 (*Metwally v University of Wollongong* (1984) 158 CLR 447).[20] Similarly, the Western Australian Premier referred the Committee to the invalidation of NSW's anti-discrimination law for inconsistency with the Commonwealth *Racial Discrimination Act 1974* (*Viskauskas v Niland* (1983) CLR 280, *Metwally v University of Wollongong* (1984) 158 CLR 447).[21] The Western Australian Premier argued that, in light of existing

15 Premier of Western Australia, *Submission 11*, p. 3.

16 Ms Sarah Chidgey, Assistant Secretary, Criminal Law and Law Enforcement Branch, Criminal Justice Division, Attorney-General's Department, *Committee Hansard*, Canberra, 1 August 2011, p. 32.

17 Premier of Western Australia, *Submission 11*, p. 2.; Victorian Attorney-General, *Submission 14*, p. 2; Dr Gans, *Submission 2*, p. 2.

18 NSW Government, *Submission 23*, p. 3.

19 Dr Jeremy Gans, *Submission 2*, p. 2.

20 Dr Jeremy Gans, *Submission 2*, p. 2; *Metwally v University of Wollongong* (1984) 158 CLR 447.

21 Premier of Western Australia, *Submission 11*, p. 4.

jurisprudence on retrospectivity, an invalidation of State cybercrime law may mean that a State Parliament is prevented from enacting new offences that take a stronger stance.[22]

6.21 It was also argued that the full impact of *Dickson's Case* is yet to be determined and the High Court's pending decision in *Momcilovic v The Queen* may help clarify the law in this area. The Committee was told that *Momcilovic v The Queen*, was part heard on 8-10 February 2011, and further heard on 7 June 2011.[23] The judgment is forthcoming, and is expected in the latter half of 2011.[24]

6.22 The Governments of Victoria, WA and NSW have asked the Commonwealth not to proceed with the Bill and accession to the European Convention until the High Court has clarified the matter. The Attorney General of Victoria submitted that:

> Until the High Court's approach to the criteria for identifying inconsistency in the area of overlapping State and federal criminal offences is made clearer, the prudent course would be for the Commonwealth Parliament to avoid risking unintended consequences by expanding the scope of the Commonwealth criminal law without yet knowing the effects of such a step.[25]

6.23 Similarly, the New South Wales Government submitted that obligations can be met based on the laws of Australia's constituent States and Territories. The New South Wales Government argues, therefore, that Australia should meet its obligations through amendment (if necessary) of State and Territory laws, if accession is considered an urgent priority.[26]

Committee View

6.24 The Committee acknowledges that none of the States or Territories objected to Australia's accession to the European Convention. The primary concern of some States relates to the impact of unrestricted national offences. Also, that as a matter of international law, all the legislative steps to meet Australia's obligations under the Convention may be undertaken

22 Premier of Western Australia, *Submission 11*, p. 3.

23 Victorian Attorney-General, *Submission 17*, p. 2; Premier of Western Australia, *Submission 11*, p. 3.

24 NSW Government, *Submission 23*, p. 4.

25 Victorian Attorney-General, *Submission 14*, p. 2.

26 NSW Government, *Submission 23*, p. 4.

under either Commonwealth or State and Territory or a combination of both.

6.25 Nonetheless, some of the evidence to the Committee indicates a continuing concern about the impact on the validity of state law of comprehensive computer offences at the federal level. Without a detailed analysis of all state provisions, the Committee is not in a position to draw any conclusion on the extent of the problem, other than to note that it may be significant.

6.26 It is likely, but not guaranteed that the High Court will clarify and remove the uncertainty caused by *Dickson's Case* in its forthcoming judgment in *Memoclovic v The Queen*. It seems prudent for the Attorney-General to consult with the States as soon as the judgment has been handed down.

7

Reporting and Oversight

Introduction

7.1 This Chapter discusses aspects of the Cybercrime Legislation Amendment Bill 2011 (the Bill) that provide for the extension of record keeping, oversight and reporting in relation to the new mechanisms for preservation notices, access to stored communications by foreign countries, and disclosures by the Australian Federal Police (AFP) of telecommunications data to foreign countries.

Cybercrime Legislation Amendment Bill

7.2 The Bill extends the existing recording keeping obligations under existing Chapter 3 (stored communications warrants) of the *Telecommunications (Interception and Access) Act 1979* (TIA Act) to preservation notices, revocations and evidentiary certificates. Proposed section 150A requires the Ombudsman to inspect an agency's records to ascertain whether the agency has kept those records.[1]

7.3 Proposed section 158A gives the Inspector General of Intelligence and Security the function of inquiring into and conducting inspections of the

---

1 The provision has been drafted in line with existing section 152 of the *Telecommunications (Interception and Access) Act 1997* (TIA Act) which requires the Ombudsman to inspect agency records to ascertain compliance with section 150 (records of destruction of product) and section 151 (Records relating to the issue of warrants).

preservation notice scheme as it applies to the Australian Security Intelligence Organisation (ASIO);

7.4 Existing sections 161 and 162 of the TIA Act require the Minister to report annually to Parliament on the use of stored communications warrants, including the number of applications for warrants and renewal applications made during the year and how many warrants included special conditions or restrictions relating to access to stored communications.

7.5 The Bill proposes to insert new section 161A into the TIA Act to expand the annual reporting obligations for enforcement agencies to include statistics on the number of preservation and revocation notices issued. In the case of the AFP, annual reporting is also expanded to include statistics about foreign preservation notices and revocations.

7.6 The Bill also proposes to insert new paragraphs into section 162(1) to require the Attorney-General to include statistics on the number of mutual assistance applications for a stored warrant and, for each foreign offence, the equivalent Australian offence in his annual report under the TIA Act.

7.7 The authorisations mechanism under Chapter 4 of the TIA Act is not subject to the same reporting and oversight mechanism:

- Section 185 of the TIA Act requires the head of an enforcement agency to retain each authorisation for three years;
- Section 186 requires the AFP to report to the Minister on the number of authorisation made, as well as any other matter requested by the Minister.

7.8 The Bill proposes to insert new subsection 185(1) that will require the Commissioner of the AFP to retain an authorisation for disclosure of telecommunications data to a foreign country for three years. Proposed new paragraph 186(1) (ca), will require the AFP to report on the number of authorisations in relation to a foreign country.

Commentary

Effective and purposeful oversight

7.9 As mentioned above, under the Bill, agencies that have issued preservation notices are required to keep certain records for inspection by the Commonwealth Ombudsman. The records are any preservation

notices, revocations and evidentiary certificates issued by the agency. The Bill requires that the Ombudsman inspect an agency's records in order to ascertain whether the agency has kept those records.

7.10 The Ombudsman submitted that, while the drafting of the Bill is in line with existing inspection and audit provisions, taken literally his role would be restricted to determining whether an agency has kept the records required, rather than allowing him to verify the veracity of these records.[2] However, under section 153(3) of the Act, the Ombudsman is empowered to report on agency compliance with a provision of the Act other than sections 150 and 151 (and also s.150A under the Bill).[3]

7.11 The Ombudsman said that to enable more effective and purposeful oversight:

> ...we have taken a broader view of our role based on the documents available under ss. 150 and 151. Our audit criteria also involve checking that:
>
> - warrants are compliant with the Act;
> - any warrant conditions imposed by issuing officers are adhered to;
> - lawfully accessed information was only communicated to authorised officers;
> - warrants are validly executed; and
> - the use of stored communications product is in accordance with the Act.[4]

7.12 The Ombudsman recommended that to remove any doubt, the Act could provide for a broader scope of the Ombudsman's oversight function – to ascertain agency compliance with Chapter 3 of the Act.

Foreign preservation notices

7.13 The Ombudsman's oversight function will include over foreign preservation notices. The Ombudsman said that his office would not simply look to see whether or not the records had been kept, but would also check the records against proposed sections 107N to 107S of the Bill, to determine if the issuance and revocation of the foreign preservation notices comply with the Act.[5]

---

2 Commonwealth Ombudsman, *Submission 15*, p. 4.
3 Commonwealth Ombudsman, *Submission 15*, p. 4.
4 Commonwealth Ombudsman, *Submission 15*, p. 4.
5 Commonwealth Ombudsman, *Submission 15*, p. 4.

> In order to do this, we may require access to certain records such as the written request from a foreign country to the AFP under s 107P (2). Although the Ombudsman may seek access if he determines that the information is relevant to an inspection,[6] we would prefer a clear mandate to access the documents under the Act. A corresponding obligation should also be placed on the AFP to keep the records.

Inspection of carrier's access, storage and disclosure of communications

7.14 In Chapter Eight, the privacy and data handling obligations of carriers is discussed. The Ombudsman argued that there was no reason why handling and destruction obligations imposed on the law enforcement agencies, should not also apply to carriers. The Ombudsman argued that:

> ... there appears to be a *gap in accountability* when carriers' actions are perhaps equally important to those of agencies in giving effect to a stored communications warrant under the Act or preservation notices under the Bill.[7]

7.15 The Ombudsman's role is to inspect an enforcement agency's records to ensure compliance with the Act. This role does not extend to inspecting the records of carriers. Although the Ombudsman can rely on his coercive powers under section 9 of the *Ombudsman Act 1976* to require a carrier to provide its records, these powers would be relied on only to assist the Ombudsman in his inspections of the enforcement agencies.

7.16 In oral evidence to the Committee, the Ombudsman expressed concerns about aspects of the current legality of information that is accessed by agencies under the laws.[8] The Ombudsman submitted that there is a lack of visibility of carrier's actions, and at times, his office was not able to ascertain if stored communications were lawfully accessed when information regarding access is held by carriers.[9]

7.17 The Ombudsman submitted that there needs to be a clear legislative mechanism to hold carriers accountable for their actions in enabling the execution of stored communications warrants.[10] There is a role for the

---

6 See section 154 of the TIA Act and the *Ombudsman Act 1976.*

7 Commonwealth Ombudsman, *Submission 15*, p. 6.

8 Commonwealth Ombudsman, *Committee Hansard*, Canberra, 1 August 2011, p. 1.

9 Commonwealth Ombudsman, *Submission 15*, p. 6.

10 Commonwealth Ombudsman, *Submission 15*, p. 6.

Information Commissioner, but, that office does not have any capacity to undertake inspections.[11]

7.18 The point was emphasised:

> I am somewhat perplexed that in the fortnight of conversations around the *New of the World* accessing phone records and Australia talking about significantly tightening up access to information we have at the same time this bill, the philosophy of which one can quite understand but which is imprecise about a lot of these details and which lowers the threshold quite materially for access to information of a highly sensitive and controversial nature and places that access outside the protections of inspections by the Ombudsman of agencies who obtain this information.[12]

Disclosures to foreign countries

7.19 Various submitters expressed concern about the inability of Australian authorities to prevent the misuse of sensitive personal information (content and traffic data) by foreign agencies. Mr Bruce Arnold and Ms Skye Masters argued that sharing information with overseas entities may be imperative, but there are 'uncertainties and scope for abuse that cannot be addressed in Australia'.[13] The Australian Privacy Foundation said that the oversight mechanisms relating to the use of disclosed information are inadequate.[14]

7.20 The Law Council of Australia argued that under the existing provisions of the TIA Act, where a stored communications warrant is issued in the context of a domestic investigation, the agency which obtains the warrant is required to capture and report on information about the number and type of arrests made, prosecutions instituted and convictions secured as a result of the information obtained under the warrant:

> This type of reporting is useful in allowing review and scrutiny of whether the information provided, and claims made, in warrant applications were actually borne out by the results obtained.[15]

---

11 Mr Nigel Waters, Board Member, Australian Privacy Foundation and Privacy International, *Committee Hansard*, Canberra, 1 August 2011, p. 7.

12 Mr Nigel Waters, Australian Privacy Foundation and Privacy International, *Committee Hansard*, Canberra, 1 August 2011, p. 7.

13 Mr Bruce Arnold and Ms Skye Masters, *Submission 18*, p. 5.

14 Australian Privacy Foundation, *Submission 16*, p. 10.

15 Section 163 of the TIA Act; Law Council of Australia, .*Submission 5*, p. 6.

7.21 The same reporting requirements are not proposed in relation to stored communications warrants issued in the context of a foreign investigation. The Law Council of Australia proposed that, if foreign agencies seek access to intrusive investigative powers, it would appear reasonable to require that they provide feedback data on how they have used the information obtained:

> Only in this way can Australian authorities satisfy themselves, on an ongoing basis, about the reliability, necessity and likely utility of future warrant requests.[16]

7.22 In relation to disclosure of telecommunications data under Chapter 4 of the TIA Act, it was suggested that reporting to the Minister by the AFP include a breakdown by country. This would provide accurate public information on the pattern of cooperation, and which countries have received telecommunication data, how often and in relation to how many Australians, or people resident in Australia.[17]

Committee View

7.23 The Committee is assured by the extension of reporting and oversight mechanism that already exist to the proposed new mechanism. There was an understandable concern about the disclosure of sensitive personal information (content and traffic) to foreign countries, where there is no restriction on the countries Australia may cooperate with. Clear statutory conditions for disclosure will assist.

7.24 However, in the Committee's view, it is impracticable to obtain detailed information about the utility of such data to a future prosecution overseas. In relation to AFP authorised disclosures, it is reasonable that something more than statistics is provided. The reporting could easily identify the countries that have received historic or existing telecommunications data without jeopardising any investigation or the privacy of any individual. Without such reporting, neither the Attorney-General nor the public will know with which countries the police are cooperating.

7.25 Clarifying the role of the Ombudsman in ascertaining compliance with the TIA Act, and not merely the retention of specified records, would also allay some of the concern about robustness of oversight. Whether the Ombudsman should have an extended jurisdiction to inspect the record

16 Law Council of Australia, *Submission 5*, p. 6.

17 Mr Bruce Arnold and Ms Skye Masters, *Submission 18*, p. 4.

keeping and compliance of private carriers are larger public policy questions. The issue may not be resolved in relation to this particular Bill, but it warrants consideration and consultation with industry and other relevant stakeholders.

Recommendation 9

That proposed new paragraph 186(1) (ca) of the *Telecommunications (Interception and Access) Act 1979* be amended to require that the Australian Federal Police report to the Minister:

- **the number of authorisations for disclosure of telecommunications data to a foreign country;**
- **identify the specific foreign countries that have received data;**
- **the number of disclosures made to each of the identified countries; and**
- **any evidence that disclosed data has been passed on to a third part or parties.**

8

Industry Data Handling and Privacy Obligations

Introduction

8.1 This Chapter addresses the privacy obligations of carriers and carriage service providers in relation to the traffic and content data retained on behalf of law enforcement and intelligence agencies.

8.2 Issues relating to the practical implementation of the provisions of the Bill and cost recovery for expenses associated with physically preserving information are dealt with in a separate chapter.

Existing obligations to assist law enforcement

8.3 The proposed preservation mechanism described in Chapter 3 provides a legislative basis for arrangements currently in place between enforcement agencies and carriers to preserve stored communications to prevent them from being deleted from the carriers' systems as a matter of routine system administration.[1]

8.4 The new requirements under the Bill to preserve data; provide access to stored communications and telecommunications data (historic and ongoing) will trigger the obligation of carriers under existing section 313 of the *Telecommunications Act 1979*. Section 313 requires the industry to provide such help as is reasonably necessary for the enforcement of the

1 See Commonwealth Ombudsman, *Submission 15*, p. 2.

criminal law, protecting the public revenue and safeguarding national security.

8.5 The new preservation regime, for example, will require carriers to collect, retain and protect the integrity of data until the notice is revoked or a period of 90 days elapses, whichever is the earlier. This will include collection and retention on behalf of a foreign country until a formal mutual assistance request has been agreed to by the Attorney General.

Commentary

8.6 The Commonwealth Ombudsman observed that carriers already play a vital role in enabling enforcement agencies to obtain stored communications under a warrant:

> Likewise, under the proposed amendments, carriers would undertake an important function in assisting agencies to comply with their legislative obligations – for example, acting in accordance with the preservation notice and not preserving product that is not covered by the notice.[2]

8.7 The Committee's attention was drawn to the lack of direction in the Cybercrime Legislation Amendment Bill 2011 (the Bill) relating to the copying, retention or destruction of preserved stored communications by carriers or carriage service providers.[3] The Explanatory Memorandum to the Bill simply states that during the period of the preservation notice, the carrier must maintain the integrity of the preserved information, and, once a preservation notice ceases to be in force, the carrier may delete the preserved information.[4]

8.8 The Committee sought specific advice from Telstra on how communications data is handled:

> Telstra retains a copy of the relevant lawful request issue on it and its response in accordance with its Document Retention Policy which, in this case, requires the information to be retained for 7 years and then destroyed.[5]

---

2 Commonwealth Ombudsman, *Submission 15*, pp. 5-6.

3 NSW Council of Civil Liberties, *Submission 21*, p. 7; Commonwealth Ombudsman, *Submission 15*, p. 5.

4 Explanatory Memorandum, Cybercrime Legislation Amendment Bill 2011, p. 10

5 Telstra Corporation Limited, *Supplementary Submission*, 14.1

8.9 The Ombudsman submitted that, in contrast to the preservation regime, existing section 150 of the *Telecommunications (Interception and Access) Act 1979* (TIA Act) places an obligation on enforcement agencies to destroy information or records obtained under a stored communications warrant when the information or record is not longer required.[6] A similar provision applies to original (but not copies) of intercept material (section 79A).[7] The Ombudsman argued that if the obligation is placed on the agencies, then the same obligation should also apply to carriers.[8]

8.10 Importantly, the Ombudsman informed the Committee that:

> The lack of visibility of carriers' actions has affected our recent inspections of enforcement agencies' stored communications records. As carriers are responsible for physically accessing stored communications under a warrant, at times, we were not able to ascertain if stored communications were lawfully accessed when information regarding access is held by carriers.[9]

8.11 The Attorney-General's Department relied on the general framework of existing privacy law. Ms Catherine Smith, First Assistant Secretary, Telecommunications Surveillance Law Branch, said:

> We are aware that the carriers are subject to the Privacy Act and as such information has to be protected. We also understand that they keep certain information for their own business purposes, which completely sits outside obviously law enforcement access. Our understanding under this new preservation regime is that, once the information is passed over to the agency if they obtain a warrant, then they should no longer have a need to have that information. They are likely to have passed over their only copy of it. We are not aware how they intend to do it in practice.[10]

8.12 It was further said that carriers bound by the *Privacy Act 1998* (Privacy Act) are obliged to destroy information that they no longer have for the purpose for which it was collected. The obligation to destroy data is connected to the initial reason why it was collected. If the data remains relevant for a legitimate business purpose it may be legitimately held after

6 Section 150 makes no distinction between originals and copies.

7 The Blunn Report noted that it was 'curious' that the requirement to destroy a record under s.79 did not extend to copies of the record; A Blunn, *Report of the Review of the Regulation of Access to Communications* (2005), Attorney-General's Department., para. 9.4.

8 Commonwealth Ombudsman, *Submission 15*, p. 5.

9 Commonwealth Ombudsman, *Submission 15*, p. 6.

10 Ms Catherine Smith, Assistant Secretary, Telecommunications Surveillance Law Branch, Attorney-General's Department, *Committee Hansard*, Canberra, 1 August 2011, p. 26.

expiration of a notice. There is no specific period mandated, and, the Committee was told that it is not a requirement of the European Convention, which is the Bill's main purpose.[11]

8.13 The Privacy Act does not contain provisions specific to the telecommunications industry. However, since the Privacy Act was extended to the private sector, the National Privacy Principles do indeed apply to the industry. It was noted, however, by several submitters that a large number of smaller Internet Service Providers (ISPs) are classified as 'small business operators' and current exempt from the obligations of the Privacy Act.[12] The Cyberspace Law and Police Centre argued that, if smaller ISPs are expected to implement real time interception capabilities and be compelled to preserve data, it is critical that they also be bound by the National Privacy Principles.[13]

8.14 The Centre also argued that the privacy jurisdiction of the Information Commissioner is inadequate:

> To provide safeguards for Australian internet users in particular, questions about enforceability of decisions and the power to impose fines on ISPs and others where there are unwarranted, unjustified and unauthorised breaches of internet user's privacy should be addressed as part of the package.[14]

8.15 The Bill, according to the Centre, should be part of a wider review, especially in light of the current debate on privacy and renewed discussion a statutory tort of privacy.[15] In this regard, the Committee's attention was drawn to the extensive work of the Australian Law Reform Commission (ALRC), which has recommended that federal law should provide for a private cause of action where an individual has suffered a serious invasion of privacy.[16]

8.16 In 2008, the ALRC conducted a major review of Australian privacy law and practice. The ALRC received a large volume of submissions in relation

---

11 Ms Catherine Smith, Attorney-General's Department, *Committee Hansard*, Canberra, 1 August 2011, p. 26.

12 Cyberspace Law and Policy Centre, *Submission 20*, p. 3.

13 Cyberspace Law and Policy Centre, *Submission 20*, p. 3. See the National Privacy Principles at Schedule 3, *Privacy Act 1988*.

14 Mr David Vaile, Executive Director, Cyberspace Law and Policy Centre, *Committee Hansard*, Canberra, 1 August 2011, p.13.

15 Mr David Vaile, Cyberspace Law and Policy Centre, *Committee Hansard*, Canberra, 1 August 2011, p.13.

16 Mr David Vaile, Cyberspace Law and Policy Centre, *Committee Hansard*, Canberra, 1 August 2011, p.13.

to telecommunications and recommended that a specific review of the TIA Act be conducted.[17] The ALRC also commented on the lack of enforcement through the criminal law and suggested that enforcement could be improved if unlawful disclosure of communications attracted a civil penalty in addition to a criminal penalty.[18]

Context of European law

8.17 Several submitters argued that the Convention on Cybercrime has to be read in the context of the legal framework that applies to Council of Europe Countries.[19]

8.18 The Privacy Foundation advised that all Council of Europe Members are parties to the Council of Europe Convention on Data Protection (CoE Convention 108), requiring adherence to international standards of data protection.[20] Most are also parties to the Additional Protocol to that Convention, which requires a data protection authority and protection of privacy in data exports.[21]

8.19 The Foundation said that:

> Since 2008 the Council of Europe has actively encouraged non-European states to become members of the Convention 108, in much the same way as it encourages non-European states to join the Cybercrime Convention. Uruguay is poised to become the first non-European state to do so.[22]

8.20 The Foundation submitted that one of the protections that should be adopted as part of Australian becoming a party to the European Cybercrime Convention is that Australia should also apply to become a party to Convention 108 and its Additional Protocol.[23] The Convention, among other things, set out obligations for the protection of privacy of data in trans-border data flows and rights of data subjects. It has been

17 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice* (ALRC 108, 2008), Recommendation 71–2.

18 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Recommendation 71–3; The Australian Communications and Media Authority should develop and publish enforcement guidelines setting out the criteria upon which a decision to pursue a civil or a criminal penalty is made.

19 Australian Privacy Foundation, *Submission* 16, p. 1. See also Queensland Council for Civil Liberties, *Submission 12*; Uniting Church in Australia, *Submission 13*.

20 Australian Privacy Foundation, *Submission 16.1*, p. 1.

21 Australian Privacy Foundation, *Submission 16.1*, p. 2.

22 Australian Privacy Foundation, *Submission 16.1*, p. 2.

23 Australian Privacy Foundation, *Submission 16.1*, p. 2.

ratified by 40 European countries and has been in operation for 30 years. Convention 108 is currently under active discussion with a view to its modernisation.[24]

8.21 In addition, a central piece of legislation in the European context is Directive 95/46/EC, which regulates the protection of individuals with regard to processing and free movement of personal data. In the particular context of the telecommunications sector, Directive 97/66/EC applies. This Directive establishes the obligation to delete data as soon as its storage is no longer necessary.[25] Directive 2002/58/EC concerns the processing of personal data and the protection of privacy in the electronic communications sector, and is usually referred to as the "ePrivacy Directive". It covers processing of personal data and the protection of privacy in the electronic communications sectors, and regulates areas such as confidentiality, billing and traffic data, rules on spam.[26]

Committee View

8.22 It became clear during the public hearing that the Bill relies on existing and separate privacy law and that no specific attention was paid in the Bill to the practical handling of content or traffic data by carriers and carriage service providers. The existing Privacy Act regime does apply, so this is not entirely surprising or indicative of any major deficiency.

8.23 However, it is common ground that telecommunications technology has changed rapidly over the past decade, which provides a justification for the Bill and accession to the Convention. Several submitters have pointed out that data protection laws are well developed in the European context, and the adapting Australian law to meet the requirement of the European Convention should have regard to this wider legal policy framework.

8.24 On the one hand, the Bill gives a clear legislative basis the preservation of communications but, on the other, does not balance this expansion with specific attention to data handling issues. There are an expanding number of carriers and carriage service providers in the Australian market place

24 See Council of Europe Data Protection, <http://www.coe.int/t/dghl/standardsetting/dataprotection/Default_en.asp> accessed 8 August 2011.

25 *Explanatory Report to the Convention on Cybercrime*, para.154, p. 27.

26 The Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters is also relevant. Its content is also based on Convention 108, but differs from Directive 95/46/EC subject coverage.

that must cooperate in law enforcement agencies and retain data under the Bill. It seems logical that any increase in the volume of retained data will inevitably increase the risk of data theft.

8.25 The Bill is an opportunity to provide:

- clarity for carriers and carriage service providers about their obligations;
- establish principles to promote confidence among the public and clarity in the event of a data breach by carriers and carriage service providers; and
- accountability to the Ombudsman and Inspector General of Security and Intelligence, whose role it is to oversight this very sensitive area of public policy on behalf of the public.

8.26 The specific challenge of privacy and new technologies has been recognised in Australia but is yet to be addressed comprehensively. The ALRC has conducted extensive consultation on privacy and new technologies, and, recommended, among other things, a specific review of the TIA Act. In 2009, the Government announced a two stage response to the ALRC report. The second stage will include a response to data handling under the *Telecommunications Act 1997*.[27]

8.27 The security of data was described as 'mission central' by Telstra. A loss of confidence by consumer about the privacy of their communications is a significant business risk to the industry and, by extension, to enforcement and interception agencies. Passage of the Bill provides an opportunity to clarify the data handling and protection obligations of carriers and carriage service providers.

27 Australian Government, *Enhancing National Privacy Protection: First Stage Response to Australian Law Reform Commission Report 108*, <http://www.dpmc.gov.au/privacy/alrc_docs/stage1_aus_govt_response.pdf> accessed 8 August 2011.

Recommendation 10

That the Attorney-General consult initially with the telecommunications industry and then with relevant Ministers, statutory bodies, and public interest groups to clarify and agree on the data handling and protection obligations of carriers and carriage service providers.

Recommendation 11

That the Cybercrime Legislation Amendment Bill 2011 be amended to require carriers and carriage service providers to destroy preserved and stored communications and telecommunications data or a record of that information when that information or record is no longer required for a purpose under the *Telecommunications (Interception and Access) Act 1979* unless it is required for another legitimate business purpose.

Recommendation 12

That the exemption of small Internet Service Providers from the *Privacy Act 1988* as small businesses be reviewed by the Attorney-General with a view to removing the exemption.

9

Industry Implementation Issues

Introduction

9.1 The Committee invited comment from the communications industry on the Cybercrime Legislation Amendment Bill 2011 (the Bill) and its potential impact on their operations once enacted. Telstra responded with a submission and gave evidence at the Committee's public hearing on 1 August 2011.

Implementation Issues

Transitional period

9.2 Generally, Telstra supported the Bill and stated that the amendments will:

- assist in streamlining procedures between carriers and carriage service providers and law enforcement agencies in the preservation of stored communications; and
- enable carriers and carriage service providers to more readily recover costs incurred when responding to requests from law enforcement agencies.[1]

---

1 Telstra Corporation Limited, *Submission 14*, p. 1.

9.3 Telstra was concerned, however, that the Bill does not allow a transition period to allow carriers and carriage service providers to put in place processes and systems to allow full compliance with the legislation. Telstra feared that the lack of a transition period means that carriers and carriage service providers will be unable to:

- undertake detailed feasibility studies into the additional obligations for carriers and carriage service providers of the Bill;
- engage vendors to modify and/or provide additional equipment and determine the technical cost impacts;
- investigate any new security and privacy risks;
- allow the lead government agency, in consultation with industry, to develop and publish delivery and formatting protocols for the handover of data;
- develop the most appropriate cost recovery model with the Attorney-General's Department; and
- allocate additional funding in the carriers and carriage service providers budget cycle.[2]

European standards

9.1 During the Committee's public hearing, Mr Peter Anthony Froelich, Telstra's Domain Expert explained the importance of clarity and consistency in interface methods to ensure the security of data and ability to respond quickly to requests:

> It would be beneficial to have some reference to international agreed mechanisms for interface, and standardisation bodies such as the European Telecommunications Standards Institute publish these types of interfaces already and they are, in fact, in use in European marketplaces. Access to those international standards would reduce bespoke development in Australia, which is something that we definitely want to avoid. We do not want to develop Australian-centric solutions to these sorts of issues.[3]

9.1 In further correspondence, Telstra advised that the following European standards are relevant:

---

2 Telstra, *Submission 14*, pp. 1-2.

3 Mr Peter Anthony Froelich, Principal Domain Expert, Telstra, *Committee Hansard,* Canberra, 1 August, 2011, p. 20.

- ETSI DTR 103 690 V0.3.0 (2011-06) Lawful Interception (LI); eWarrant Interface (describes and electronic interface for workflow management between law enforcement and carriers or internet service providers (ISP's));
- ETSI TS 102 656 V1.1.2 (2007-12) Lawful Interception (LI); Retained Data; Requirements of Law Enforcement Agencies for handling Retained Data; and
- ETSI TS 102 657 V1.3.1 (2009-09) Lawful Interception (LI); Retained data handling; Handover interface for the request and delivery of retained data.[4]

9.2 These standards describe pragmatic agreed ways to interface between Agencies and Carriers/ISP's attempting to describe real world expectations for managing disclosures and coordinating information flow. Telstra expects that these standards would form part of the framework to deliver speedier responses, more resilient functions and greater cost effectiveness for both government and industry.

Cost recovery

9.3 Telstra also raised the issue of cost recovery:

> Telstra also believe that the additional obligations to preserve data are beyond Telstra's business needs and should be subject to further discussions with the government, as the proposed amendments, we believe, will place a significant resource burden on carriers and carriage service providers in the form of cost and manpower.[5]

9.4 Telstra representatives acknowledged that they did not necessarily envisage an increase in the number of requests they would receive, but sought acknowledgement that they will have to change their systems and incur costs to comply with the legislation.[6] It is likely that the largest number of preservation notices will be issued to companies that have the largest market shared. Telstra, for example, accounts for 43% of the mobile market, 73% of fixed lines, and 45% of fixed retail broadband.[7]

---

4 Correspondence, 9 August 2011.

5 Mr James Shaw, Director Government Relations, Telstra, *Committee Hansard*, Canberra, 1 August 2011, p. 17.

6 Mr James Shaw, Telstra, *Committee Hansard*, Canberra, 1 August 2011, p. 18.

7 Telstra, *Supplementary Submission 14.1*. p.1.

Telstra recommendations

9.5 Telstra recommended:

- carriers and carriage service providers be allowed to complete a compliance feasibility study prior to Royal Assent;
- having an exemption process for carriers and carriage service providers unable to comply with the short time frame;
- the exemption to include an implementation plan; and
- that implementation occur a suitable length of time (not more than 18 months) after technical requirements have been published by the Attorney-General's Department.[8]

Attorney-General's Department response

9.6 The Attorney-General's Department was surprised by Telstra's position on the required timeframe for implementation as it felt that service providers were already providing the required responses and that no new infrastructure should be required as there was no specified way that providers had to store the required communications. The Attorney-General's Department stated:

> We have been working for some time with the main players, as I said earlier, who actually provide mobile services like text messages of where the high risk is of losing that evidence or intelligence where it is needed...
>
> Certainly we are willing to talk to industry now and are talking to industry about their obligations on a daily basis as to how they can do this to best have it up and running.
>
> ... I did not understand from my discussions that there would be any need to build delivery standards or have any specifications or anything like that...There are already delivery systems in place for the delivery of this kind of information—the stored communications regime. [9]

8 Telstra, *Submission 14*, pp. 2-3.

9 Ms Catherine Smith, Assistant Secretary, Telecommunications Surveillance Law Branch, Attorney-General's Department, *Committee Hansard*, Canberra, 1 August 2011, p. 31.

Committee View

9.7 The Committee is conscious of the practical impact the introduction of the Bill will have on carriers and carriage service providers. The largest demand is likely to fall to those companies with the largest share of the market, especially in mobile services, who will in turn bear the largest overall cost.

9.8 The Committee is also conscious that introduction of the legislation may have impose a disproportionate cost on smaller carriers and carriage service providers.

9.9 There appears to be a need for greater consultation between the government and industry on the implementation of the Bill. Accordingly, the Committee agrees with the Attorney-General's Department that 'it is important that [the Department] start talking to industry very quickly on how this will be done'.[10]

Recommendation 13

That the Attorney-General's Department consult widely with carriers and carriage service providers to ensure that the Cybercrime Legislation Amendment Bill 2011, when enacted, can be implemented in a timely and efficient manner.

Senator Catryna Bilyk

Chair

10 Ms Catherine Smith, Attorney-General's Department, *Committee Hansard*, Canberra, 1 August 2011, p. 31.

Additional Comments—Senator Scott Ludlam, Australian Greens

The Cyber-Safety Committee has again proven its worth in engaging with the complex and difficult issues pertaining to online security by providing useful analysis and recommendations that validate and address some concerns of experts and stakeholders.

The Australian Greens continue, however, to believe that there are fundamental flaws in the Cybercrime Bill and the controversial European Convention on Cybercrime that it seeks to implement.

The Greens regret to agree with submissions and evidence objecting to the fast tracking of this Committee process. Setting five business days for civil society organisations that largely rely on volunteer labour to provide input, is unfair. A seven day extension, while welcome, is not good enough given the importance of the matters in question.

With this Bill the Attorney General's Department yet again seeks to fast track legislation, which yet again extends well beyond its nominal purpose, to yet again encroach upon on the civil liberties of Australians in the name of law enforcement and counter-terrorism. The Attorney General's track record in this regard is demonstrated through numerous amendments to the Telecommunications Act, Intelligence Services Amendments, and the woefully inadequate "reforms" the government undertook to the extreme Howard anti-terrorism laws. Once again with this Bill, a major expansion of the surveillance state is occurring with entirely inadequate justification.

Some examples of the Attorney General overreaching well beyond the requirements of the Convention:

- The preservation regime in this Bill provides for ongoing collection and retention of communications, which is not provided for by the Convention. The Ombudsman and several other submitters argued that the ongoing preservation of communications amounts to an interception, which is

governed by a specific interception warrant regime with stricter thresholds and more reporting and oversight.

- The Bill extends preservation notices to ASIO, which is not a requirement of the Convention but has been done automatically on the basis of 'interoperability' with law enforcement agencies. This was acknowledged in the report but not commented upon. ASIO's ongoing mandate creep and the unjustified expansion of its powers are worthy of comment.

- Under the Convention, police may decline to pass traffic data where the offence is a political offence or is otherwise inconsistent with fundamental values and human rights standards. This is not reflected in the Bill. The Convention does not require States parties to lower their own standards.

- The Bill allows the AFP to require a carrier(s) to preserve traffic data on an ongoing basis on behalf of a foreign country in response to a mutual assistance request. The ongoing preservation of traffic data is not provided for in the Convention.

- The retention of the traffic data may be for up to 180 days, although this is not required by the Convention. The extended period is said to accommodate the slowness of mutual assistance processes. The Australian Privacy Foundation argued that 180 days is excessive and twice that required by the Convention.

The following improvements should be made to the Bill

- The Greens do not believe Recommendation 6 goes far enough to uphold Australia's opposition to the death penalty. The disclosure of telecommunications data to a foreign country in relation to an offence that carries the death penalty should be refused in the absence of an assurance that the foreign country that the death penalty will not be imposed or carried out. As it stands, Recommendation 6 leaves the door open for Australian law enforcement agencies to directly or inadvertently support an overseas prosecution which would lead to an execution. This is completely unacceptable.

- The Ombudsman has asked that his powers to inspect and audit compliance with the preservation regime be clarified to ensure he can check compliance with the Act and not mere record keeping. This request was not dealt with by the Committee but should be addressed through amendments when the Bill is debated.

- Preservation of data is a new mechanism. It will require carriers to retain communications and traffic data at least until a stored communication warrant is obtained. There is no direction in the Bill on how carriers should handle such data or the interface standards between the industry and law

enforcement agencies. The Explanatory Report to the Council of Europe Convention on Cybercrime makes a point of stating that the cybercrime treaty is not about retention but about targeted law enforcement. In May 2001 the European Data Protection Supervisor issued an opinion concluding that the European directive on data retention is incompatible with the EU Charter of Fundamental Rights (art. 7 and 8).

- The Bill allows the AFP to pass traffic data obtained for a domestic investigation directly to foreign counterparts without the need for any request. Thus a secondary disclosure may be proactive. The is no restriction on the number or type of countries that may receive traffic data from the AFP.

- There is no independent oversight of compliance with police authorised disclosures, and none envisaged in relation to disclosure to foreign counterparts. It may be difficult to make oversight meaningful in this context. However, it is possible that authorisations could be reviewed from a fundamental human rights perspective, which the Greens believe is preferable.

- The European Convention exhaustively defines traffic data. In contrast, the Bill relies on the principal Act and does not use Convention terminology. It is impossible therefore to say whether 'telecommunications data' in the TIA Act (which is defined rather indirectly as 'non-content data') is the same at the Convention definition of 'traffic data'. This does not present any difficulty for accession to the Convention. It does present a problem for citizens who wish to know what the law is.

- The Australian Privacy Foundation argued that the preservation regime in the Bill (Chap 3 TIA Act) does not require law enforcement agencies to make a decision as to whether telecommunications data (as opposed to content of communications) may be sufficient. It is possible to amend the Bill to require them to make that decision. In practice, however, it is likely that police will go for telecommunications data if it is sufficient because there are no warrant requirements (Chapter 4 of the TIA Act). A statutory signal would make privacy advocates more confident there will be grounds in the future for holding law enforcers to account if they exceed 'necessity and proportionality test'. Such a provision would provide a basis for argument in later proceedings.

- The threshold offence is determined by reference to the foreign country's law and does not require dual criminality as a precondition either to mutual assistance (discretionary) or for issuing the stored communications warrant. The Australian Privacy Foundation recommended that proposed section 5EA incorporate a dual criminality test, to at least ensure there is some comparable offence in both Australia and the foreign country. This

was not picked up by the Committee but is worthwhile as a secondary protection that can be exercised by the 'issuing authority'.

The Australian Law Reform Commission has recommended that the Telecommunications Interception Act be reviewed in its entirety – a proposition strongly supported by the Greens. The TIA Act has been subject to numerous amendments. It is technically difficult and would benefit from 'post enactment review' by a parliamentary committee or independent review by the ALRC. The more technically difficult an Act is the more likely there is to be uncertainty about obligations, mistakes and misinterpretation. Telecommunications is supposed to be part of the second stage review of Australian privacy law but Government's progress has been delayed. Perhaps the Attorney's appetite for undue haste could be exercised in this direction.

The Australian Greens believe that the Committee has proposed substantive amendments that the government must act upon. These additional comments have proposed further improvements to the Bill. It is our strong view that the government not proceed until these combined amendments have been drafted and thoroughly debated.

Senator Scott Ludlam

A

Appendix A — Submissions

1	Civil Liberties Australia (CLA)
2	Dr Jeremy Gans
3	Law Institute of Victoria
4	Council of Europe
5	Law Council of Australia
6	Brilliant Digital Entertainment
7	South Australia Police
8	Electronic Frontiers Australia Inc
9	Australian Bar Association
10	Office of the Australian Information Commissioner
11	Premier of Western Australia
12	Queensland Council for Civil Liberties
13	Uniting Church in Australia, Synod of Victoria and Tasmania
14	Telstra Corporation Limited
14.1	Telstra Corporation Limited
15	Commonwealth Ombudsman
15.1	CONFIDENTIAL
16	Australian Privacy Foundation
17	Victorian Attorney-General
18	Mr Bruce Arnold & Ms Skye Masters

19 Mr Philip Hall

20 Cyberspace Law and Policy Centre

21 NSW Council for Civil Liberties

22 Office of the Privacy Commissioner NSW

23 NSW Government

B

Appendix B — Witnesses

Monday, 1 August 2011 - Canberra

Attorney General's Department

Ms Sarah Chidgey, Assistant Secretary, Criminal Law and Law Enforcement Branch

Mr David Cramsie, Senior Legal Officer

Mr Andrew Kiley, Senior Legal Officer

Ms Catherine Smith, Assistant Secretary, Telecommunications and Surveillance Law Branch

Australian Federal Police

Assistant Commissioner Neil Gaughan, National Manager, High Tech Crime Operations

Ms Elsa Sengstock, Coordinator, Legislation Program

Australian Privacy Foundation

Dr Roger Clarke, Chairman

Mr Nigel Waters, Board members

Australian Security Intelligence Organisation

Deputy Director-General David Fricker

Cyberspace Law and Policy Centre

Mr Chris Connolly, Research Associate

Mr David Vaile, Executive Director

Law Council of Australia

Ms Rosemary Budavari, Co-Director, Criminal Law and Human Rights

Telstra Corporation Ltd

Mr Peter Froelich, Principal Domain Expert

Mr James Shaw, Director Government Relations

C

Appendix C – Enforcement Agencies

Agencies that are able to apply for stored communications warrants fall within the definition of 'enforcement agency' in the *Telecommunications (Interception and Access) Act 1997* (TIA Act). An enforcement agency is defined as:

> ***enforcement agency*** means:
>
> (a) the Australian Federal Police; or
>
> (b) a Police Force of a State; or
>
> (c) the Australian Commission for Law Enforcement Integrity; or
>
> (d) the ACC; or
>
> (e) the Crime Commission; or
>
> (f) the Independent Commission Against Corruption; or
>
> (g) the Police Integrity Commission; or
>
> (h) the Office of Police Integrity; or
>
> (i) the Crime and Misconduct Commission; or
>
> (j) the Corruption and Crime Commission; or
>
> (k) an authority established by or under a law of the Commonwealth, a State or a Territory that is prescribed by the regulations for the purposes of this paragraph; or
>
> (l) a body or organisation responsible to the Ministerial Council for Police and Emergency Management - Police; or
>
> (m) the CrimTrac Agency; or
>
> (n) anybody whose functions include:
>
> (i) administering a law imposing a pecuniary penalty; or

(ii) administering a law relating to the protection of the public revenue.

The Australian Customs and Border Protection Service has been prescribed for the purposes of paragraph (k).

Agencies that can authorise the disclosure of existing non-content information

The TIA Act enables an enforcement agency (as defined above) to authorise the disclosure of non-content information that is in existence at the time an authorisation is made under Chapter 4 of the TIA Act.

The proposed amendments allow the Australian Federal Police to authorise a disclosure of existing information for the enforcement of the criminal law of a foreign country.

A broad range of agencies have authorised the disclosure of this information. While the vast majority of authorisations are made by interception agencies and criminal law enforcement agencies, the Annual Report tabled in Parliament indicates other agencies use this information, including:

- Australian Taxation Office
- Centrelink
- Department of Commerce – Office of Fair Trading (New South Wales)
- Department of Immigration and Citizenship
- Department of Primary Industries (Victoria), and
- Insolvency and Trustee Service Australia

Agencies that can authorise the disclosure of non-content information on a prospective basis

The TIA Act enables 'criminal law enforcement agencies' to authorise the disclosure of non-content information on a prospective basis under Chapter 4 of the TIA Act.

A 'criminal law enforcement agency' is defined as an agency covered by paragraphs (a)-(k) of the definition of enforcement agency and so is:

(a) the Australian Federal Police; or

(b) a Police Force of a State; or

(c) the Australian Commission for Law Enforcement Integrity; or

(d) the ACC; or

(e) the Crime Commission; or

(f) the Independent Commission Against Corruption; or

(g) the Police Integrity Commission; or

(h) the Office of Police Integrity; or

(i) the Crime and Misconduct Commission; or

(j) the Corruption and Crime Commission; or

(k) an authority established by or under a law of the Commonwealth, a State or a Territory that is prescribed by the regulations for the purposes of this paragraph.

The Australian Customs and Border Protection Service has been prescribed for the purposes of paragraph (k) and is the only agency without interception powers to have made an authorisation in the most recent reporting year.

D

Appendix D – Interception Agencies

The *Telecommunications (Interception and Access) Act 1997* (TIA Act) sets an exhaustive list of agencies that can apply for telecommunications interception warrants.

Commonwealth agencies are listed in the definition of 'interception agency' in the TIA Act, which enables them to apply for interception warrants.

State and Territory agencies are initially included within the definition of 'eligible authority', which enables them to receive lawfully intercepted information, but not apply for interception warrants. In order for the eligible authority to be declared an interception agency, the Attorney-General makes a declaration under s. 34 of the TIA Act. This can be done after the Attorney-General is satisfied that the preconditions for declaration, set out in s. 35 of the TIA Act are in place. These include that appropriate relevant State laws are in place. The agencies which can currently apply for interception warrants are:

- ASIO
- Australian Federal Police
- Australian Crime Commission
- Australian Commission for Law Enforcement Integrity
- Queensland Police Service
- Crime and Misconduct Commission (Queensland)
- New South Wales Police Force
- New South Wales Crime Commission
- Police Integrity Commission (New South Wales)

- Independent Commission Against Corruption (New South Wales)
- Victoria Police
- Office of Police Integrity (Victoria)
- Tasmania Police
- South Australia Police
- Western Australia Police
- Corruption and Crime Commission (Western Australia), and
- Northern Territory Police Force

E

Appendix E – Framework for Access to Communications in Australia

	Disclosure of Historic Non-Content Data	Prospective Disclosure Non-Content Data	Stored Communications	Telecommunications Interception
What type of information	Information about communications (but not the content of the communications themselves). The information is created in the course of a carrier's business and is in existence	The same information as historic non-content data. However, rather than authorising the disclosure of information in the carrier's possession, the authorisation enables the additional disclosure of	Stored communications are 'communications' that are stored on the equipment of carriers, are accessible by the intended recipient of the communication and can only be accessed with the	Telecommunications interception is the real-time copying or recording of information that is passing over a telecommunications system. It can be by way of a fixed landline, mobile communication or

	Disclosure of Historic Non-Content Data	Prospective Disclosure Non-Content Data	Stored Communications	Telecommunications Interception
	at the time the disclosure is authorised. It includes details about subscribes and billing and assists agencies establish who uses a service, the parties to a communication, when it was sent and received and sometimes their location.	information which comes into existence for an ongoing period.	assistance of the employee of a carrier. These communications include sent emails and sms messages as well as voicemail messages.	communications via computer networks.
Threshold for access	Either: • Security (as defined in the ASIO Act) • the enforcement of the criminal law • the enforcement of a law imposing a pecuniary penalty, or • the protection of the public revenue	Either: • Security, or • The investigation of an offence with a penalty of at least three years' imprisonment	Either: • Security, or • An offence for which telecommunications interception is available, • An offence with a penalty of at least three years' imprisonment, • An offence with a penalty of 180 penalty units for an individual, or 900 penalty units for a body corporate	Either: • Security, or • A 'serious offence', in section 5D of the Interception Act. They generally carry a penalty of at least seven years' imprisonment, however there are exceptions. Offences are included within the regime on a case-by-case amendment

	Disclosure of Historic Non-Content Data	Prospective Disclosure Non-Content Data	Stored Communications	Telecommunications Interception
Who can access it	An 'enforcement agency', as defined in section 5 of the Interception Act (an agency with the above functions). These can be Federal, State or Local Government agencies.	ASIO, or a 'criminal law enforcement agency', as defined in the Interception Act. There are both Federal and State criminal law enforcement agencies.	ASIO, or an enforcement agency.	ASIO and 16 other Commonwealth and State agencies. Commonwealth agencies are defined in the Act and State agencies are authorised by a declaration made by the Attorney-General.
How can it be accessed	The agency provides an authorisation to the carrier that holds the information authorising the disclosure of the information. For ASIO, authorisations can be made by the Director-General, Deputy Director-General or an employee authorised by the Director-General. For enforcement agencies, authorisations can be made by a person in a	The agency provides an authorisation to the carrier that holds the information authorising the disclosure of the information. For ASIO, authorisations can be made by the Director-General, Deputy Director-General or an authorised employee at the equivalent level of SES Band 2. For criminal law enforcement agencies,	An enforcement agency must apply to a Federal Judge or Magistrate, or a Nominated AAT Member for a warrant which authorises access to any stored communications held by the carrier that relate to the person named in the warrant. ASIO obtain access to stored communications as part of their telecommunications interception warrants. They do not have a	Telecommunications interception is authorised by way of a warrant. Warrants for law enforcement agencies are issued by a Judge of a Federally-created court that has consented to issue warrants. Warrants for ASIO are issued by the Attorney-General.

	Disclosure of Historic Non-Content Data	Prospective Disclosure Non-Content Data	Stored Communications	Telecommunications Interception
	management position or management office authorised by the agency head.	authorisations can be made by a person in a management position or management office authorised by the agency head.	separate means of access.	
Set out in	Interception Act – Chapter 4	Interception Act – Chapter 4	Interception Act – Chapter 3	Interception Act – Chapter 2