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.