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.