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.