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.**