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.