

Chapter 1

Introduction

1.1 On 24 June 2010, the Senate referred the matter of the adequacy of protections for the privacy of Australians online to the Senate Environment and Communications References Committee for inquiry and report by 20 October 2010. The reporting date was subsequently extended by the Senate until 22 March, 24 March, and 7 April 2011.

1.2 The terms of reference required that the committee have regard to:

- (a) privacy protections and data collection on social networking sites;
- (b) data collection activities of private companies;
- (c) data collection activities of government agencies; and
- (d) other related issues.

Reasons for this inquiry

1.3 The Senate's referral of this inquiry, on the motion of Senator Ludlam, was timely given the significant advances in online technology and computing power over the past decade, many of which have important implications for personal privacy.

1.4 For example, the rapid uptake of social networking technologies since 2002 has substantially expanded the amount and type of personal information that people are sharing online,¹ while improvements in cloud computing technology have made it possible to shift vast quantities of personal data around the world to take advantage of cheap data storage.² Technology has also made it possible for companies to monitor the way in which individuals behave online for marketing purposes. A combination of these developments, and other online technological advancements has exacerbated existing concerns with privacy protection in Australia, and in some instances created new concerns.

1.5 Conversely, online technology has also enhanced the ability of individuals and organisations to hide their personal information, including their identity, in certain circumstances. For example, it was reported in *The Age* that 'an industry has now sprung up to protect the identity of those who own dubious websites'.³ Furthermore, newer communications technologies, such as email, often allow users to remain anonymous, or do not record the same data about individual communications that was

1 Friendster was launched in 2002: www.friendster.com/info/index.php (accessed 13 December 2010); Myspace in 2003: Asher Moses, 'MySpace founder takes on Rupert', *Sydney Morning Herald Online*, www.smh.com.au/news/biztech/myspace-founder-takes-on-rupert/2006/11/08/1162661728774.html (accessed 13 December 2010); and Facebook in February 2004: www.facebook.com/press/info.php?factsheet (accessed 13 December 2010).

2 Office of the Privacy Commissioner (OPC), *Submission 16*, pp 21–34.

3 Ian McIlwraith, 'Netting web scammers', *The Age*, 16 September 2010, p. 8.

recorded with conventional technologies, such as telephones. This has created new challenges for law enforcement agencies, as the committee heard in evidence from the Australian Federal Police and Attorney-General's Department.⁴

1.6 The timeliness of the committee's examination of this matter is reflected by the fact that it coincides with a number of reviews of privacy regulation both in Australia and overseas. In June 2010, the Australian Government released an exposure draft of major amendments to the *Privacy Act 1988*, which reflect the first stage of its response to the Australian Law Reform Commission's (ALRC) report on Australian privacy law and practice.⁵ The exposure draft was referred to the Senate Finance and Public Administration Legislation Committee for inquiry and report by 1 July 2011.⁶

1.7 The committee understands that the government is also reviewing cyber security and cyber crime in response to the recent House of Representatives committee report *Hackers, Fraudsters and Botnets: Tackling the Problem of Cyber Crime*.⁷ The review will look at the practicality of implementing the recommendations of the Standing Committee's report and will focus on avenues to protect individuals, the community and the private security in the online world. Although the government's review is broader in scope than the committee's inquiry, there may be some common ground, as a secure online environment with adequate privacy will help protect people from identity theft or other online crime involving misuse of personal information.

1.8 The committee's inquiry also coincides with the European Commission's review of the general European Union legal framework on the protection of personal

4 Ms Catherine Smith, Assistant Secretary, Telecommunications and Surveillance Law Branch, Attorney-General's Department, *Committee Hansard*, 29 October 2010, pp 85–86.

5 Department of the Prime Minister and Cabinet, *Privacy Reforms*, www.alrc.gov.au/publications/report-108 (accessed 9 December 2010); Australian Law Reform Commission (ALRC), *For Your Information: Australian Privacy Law and Practice*, Report No 108, 2008, available at www.alrc.gov.au/publications/report-108 (accessed 9 December 2010); and Senator the Hon Joe Ludwig, Cabinet Secretary, *Enhancing National Privacy Protection: Australian Government First Stage Response to the Australian Law Reform Commission Report 108*, October 2009, available at www.dpmc.gov.au/privacy/alrc_docs/stage1_au_govt_response.pdf (accessed 9 December 2010)

6 For information about the Senate Finance and Public Administration Legislation Committee's inquiry see: www.aph.gov.au/Senate/committee/fapa_ctte/priv_exp_drafts/info.htm (accessed 10 December 2010).

7 House of Representatives Standing Committee on Communications, *Hackers, Fraudsters and Botnets: Tackling the Problem of Cyber Crime*, June 2010, www.aph.gov.au/house/committee/coms/cybercrime/report.htm (accessed 7 March 2011); and the government response, 25 November 2010, www.aph.gov.au/house/committee/coms/governmentresponses/cybercrime.pdf (accessed 7 March 2011).

data,⁸ as well as consideration by the Attorney-General's Department of a mandatory data retention scheme based on that adopted by the EU in 2006.⁹

1.9 Furthermore, in the United States, the Federal Trade Commission released a preliminary report in December 2010 on 'Protecting Consumer Privacy in an Era of Rapid Change' and recommended a framework for businesses and policymakers in dealing with consumer privacy issues.¹⁰

Conduct of the inquiry

1.10 In accordance with its usual practice, the committee advertised details of the inquiry in *The Australian* on 30 June 2010. The committee also contacted a range of organisations, inviting them to make submissions. The committee received 27 submissions, listed at Appendix 1.

1.11 The committee held two public hearings: in Canberra on 29 October 2010 and in Melbourne on 1 December 2010 (see Appendix 2).

1.12 The committee notes that despite several requests, Facebook failed to provide the committee with any information about its privacy policies and settings in the Australian online environment.

Report structure

1.13 This inquiry raised a diverse range of complex issues related to online technology and privacy. The issues raised were so varied and numerous that it would be impossible to adequately cover them all within the confines of a Senate Committee report. Instead, the committee has identified key themes and recurring issues and synthesised them into a discussion of the major issues confronting privacy regulators with the development of online technologies.

1.14 Broadly, the issues raised fall into two categories: those related to the adequacy of the existing privacy framework for protecting the privacy of Australians online; and challenges for law enforcement arising from technological advances.

8 European Commission, *Review of the data protection legal framework*, http://ec.europa.eu/justice/policies/privacy/review/index_en.htm (accessed 10 December 2010). The review has thus far consisted on a stakeholders' conference in May 2009 and further consultations during 2010, and a strategic communication released on 4 November 2010.

9 Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, 15 March 2006 at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF> (accessed 10 December 2010).

10 United States Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: a proposed framework for businesses and policymakers*, Preliminary FTC Staff Report, December 2010 at www.ftc.gov/os/2010/12/101201privacyreport.pdf (accessed 6 January 2010).

1.15 Chapter 2 of this report outlines the existing privacy framework in Australia, including proposed legislative amendments.

1.16 Chapter 3 discusses the first category of online privacy issues raised during this inquiry—which relate to the adequacy of current and proposed protections for Australians in the online environment. These issues include: the role of consent in Australian privacy law; the small business exemption in the *Privacy Act 1988*; behavioural advertising; the transnational nature of the internet; and whether Australia should enact a statutory cause of action for invasion of privacy.

1.17 Chapter 4 of this report considers the law enforcement challenges arising from technological advances, and specifically the Attorney-General's Department's proposed mandatory data retention scheme.

1.18 Recommendations are addressed either to the Office of the Privacy Commissioner (OPC) or to the government. The committee notes that within government, several different departments will be involved in responding, including the Department of the Prime Minister and Cabinet; the Attorney-General's Department; and the Department of Broadband, Communications and the Digital Economy.

1.19 The OPC was integrated into the Office of the Australian Information Commissioner (OAIC) on 1 November 2010. The Office's submission to this inquiry and the Privacy Commissioner's appearance before this committee both occurred before 1 November 2010, at a time when the Office of the Privacy Commissioner was a stand-alone office. For consistency the report will refer to the Office of the Privacy Commissioner.

Acknowledgments

1.20 The committee would like to thank all of the organisations, individuals and government departments and agencies that contributed to this inquiry. In particular the committee expresses its appreciation to the Attorney-General's Department and the Australian Federal Police for willingly providing the committee with confidential information regarding the proposed data retention proposal.