The Regulation of Information Privacy Protection in Electronic Commerce (E-commerce) in Australia

Thillagavathy Vijyaleximi Rajaretnam

A thesis submitted in fulfilment of the degree of

Doctor of Philosophy

Thesis submitted: January 2013

School of Law

University of Western Sydney
# Table of Contents

Table of Contents i

Acknowledgements v

Statement of Authenticity vi

List of Selected Acronyms vii

List of Diagrams and Tables viii

Publications Based on this Thesis ix

Abstract x

Chapter 1: Introduction 1

1.1 Introduction 1

1.2 E-Commerce: the Context 1

1.3 The Issue of Information Privacy for E-commerce Users 2

1.4 The Scope and Outline of the Dissertation 6

Chapter 2: Information Technology and How Privacy is Violated 9

2.1 Introduction 9

2.2 Privacy Invasive Technologies 11

2.2.1 Cookies and Related Technologies 11

2.2.2 Dataveillance/data Mining 14

2.3 Data Security 18

2.3.1 Data Security Technologies 21
# 6.2 Privacy Act and NPPs

6.2.1 Key Limitations on the Application of the Privacy Act

6.2.2 The National Privacy Principles (NPPs)

# 6.3 Conclusion

# Chapter 7: Industry Privacy Codes

7.1 Introduction

7.2 Industry Codes

7.3 Privacy Act - NPPs

7.4 Supervisory Authorities and Code Regulators

7.4.1 The Australian Securities and Investment Commission (‘ASIC’)  
7.4.2 Australian Competition and Consumer Commission (‘ACCC’)  
7.4.3 Australian Communications and Media Authority (‘ACMA’)  
7.4.4 Telecommunications Industry Ombudsman (TIO)

7.5 Telecommunications Industry Codes of Practice

7.5.1 Telecommunications Consumer Protections (TCP) Code (‘TCP Code’)  
7.5.2 Australian E-Marketing Code of Practice 2005 (‘e-Marketing Code’)

# 7.6 Conclusion

# Chapter 8: Complaints Handling, Compliance, and Enforcement

8.1 Introduction

8.2 Complaints

8.2.1 Privacy Act  
8.2.2 Complaints handling under TCP Code and the e-Marketing Code

8.3 Compliance

8.3.1 Compliance with Privacy Act NPPs  
8.3.2 Compliance with the TCP Code and the E-marketing Code

8.4 Remedies and Enforcement

8.4.1 Privacy Act
Acknowledgements

I wish to express my appreciation and thank many people for making it possible for me to have successfully completed my PhD dissertation.

I wish to first thank Professor Razeen Sappideen, my principal supervisor, and Professor Carolyn Sappideen, my co-supervisor, for their constant guidance, encouragement, and support given to me in completing this dissertation. I owe them immense gratitude. This dissertation is part of a larger argument on the right to privacy that is intermingled with other fundamental human rights and freedom that is continued to be challenged by the rapid development of information technologies. Professor Razeen Sappideen and Professor Carolyn Sappideen have continued to challenge the original position I had taken in the initial Chapters of this dissertation. This challenge forced me to better articulate and develop my positions. Their countless insights into the issues have also strengthened my understanding of privacy issues and law.

Many thanks also goes to Dr Masudul Haque, my second co-supervisor, and colleagues at the School of Law, University of Western Sydney for the encouragement given to me and for sharing their own PhD student experiences. I have also greatly benefited from the comments and feedback from colleagues when presenting my ideas at school seminars and conferences.

My appreciation and thanks goes to my niece, Sasha Mahadaven, and Dr Xiaobo Zhao, who have been assisting me with formatting and getting my thesis ready for the printers. I thank you both for giving me your time and your willingness to help.

I could not have possibly completed this dissertation without my family. I wish to thank my siblings, Anna, Shan, Saras, Kuvara, and Ganesh, and my husband, John. Your encouragement and support, and your belief in me have been invaluable. But most of all I owe all my past, present, and future achievements to the two most important persons in my life, my beloved late parents, my mother, Rajambal Kathireson Pillay, and my father, Rajaretnam Govindasamy without them I could not have come this far. It is to their memory that I wish to dedicate this work.
Statement of Authenticity

This dissertation has been presented in the fulfilment of the requirements of a PhD in Law at the University of Western Sydney. I certify that this dissertation is the result of my own work and that any assistance received in its preparation and all sources used have been acknowledged in the text. I also certify that the substance of this dissertation has not already been submitted for any degree and is not currently being submitted for any other degree.

Thillagavathy Vijyaleximi Rajaretnam
### List of Selected Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACCAN</td>
<td>Australian Communications Consumer Action Network</td>
</tr>
<tr>
<td>ACCC</td>
<td>Australian Competition and Consumer Commission</td>
</tr>
<tr>
<td>ACMA</td>
<td>Australian Communications and Media Authority</td>
</tr>
<tr>
<td>ADMA</td>
<td>Australian Direct Marketing Association</td>
</tr>
<tr>
<td>AIC</td>
<td>Australian Information Commissioner</td>
</tr>
<tr>
<td>ALRC</td>
<td>Australian Law Reform Commission</td>
</tr>
<tr>
<td>APF</td>
<td>Australian Privacy Foundation</td>
</tr>
<tr>
<td>ASIC</td>
<td>Australian Securities and Investment Commission</td>
</tr>
<tr>
<td>B2C</td>
<td>Business-to-consumer</td>
</tr>
<tr>
<td>BFSO</td>
<td>Banking and Financial Services Ombudsman</td>
</tr>
<tr>
<td>CSP</td>
<td>Carriage Service Providers</td>
</tr>
<tr>
<td>EC</td>
<td>European Commission</td>
</tr>
<tr>
<td>EFA</td>
<td>Electronic Frontiers Australia</td>
</tr>
<tr>
<td>EFTPOS</td>
<td>Electronic Funds Transfer Point of Sale</td>
</tr>
<tr>
<td>EPIC</td>
<td>Electronic Privacy Information Centre</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>FIPs</td>
<td>Fair information practices</td>
</tr>
<tr>
<td>FOI</td>
<td>Freedom of Information</td>
</tr>
<tr>
<td>FTC</td>
<td>Federal Trade Commission</td>
</tr>
<tr>
<td>GSM</td>
<td>Global Standard Mobile</td>
</tr>
<tr>
<td>HTML</td>
<td>Text Mark-up Language</td>
</tr>
<tr>
<td>HTTP</td>
<td>Hypertext Transfer Protocol</td>
</tr>
<tr>
<td>ICO (UK)</td>
<td>Information Commissioner’s Office (UK)</td>
</tr>
<tr>
<td>ICTs</td>
<td>Information and Communications Technologies</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>IPP</td>
<td>Information Privacy Principles</td>
</tr>
<tr>
<td>ISPs</td>
<td>Internet Service Providers</td>
</tr>
<tr>
<td>NAI</td>
<td>Network Advertising Initiative</td>
</tr>
<tr>
<td>NSW LRC</td>
<td>New South Wales Law Reform Commission</td>
</tr>
<tr>
<td>OAIC</td>
<td>Office of the Australian Information Commissioner</td>
</tr>
<tr>
<td>OBA</td>
<td>Online Behavioural Advertising</td>
</tr>
<tr>
<td>OECD</td>
<td>Organisation for Economic Co-operation and Development</td>
</tr>
<tr>
<td>OFPC</td>
<td>Office of the Federal Privacy Commissioner</td>
</tr>
<tr>
<td>OPC</td>
<td>Office Privacy Commissioner</td>
</tr>
<tr>
<td>OSB</td>
<td>Office of Small Business</td>
</tr>
<tr>
<td>P3P</td>
<td>Platform for Privacy Preferences</td>
</tr>
<tr>
<td>PC</td>
<td>Privacy Commissioner</td>
</tr>
<tr>
<td>PETs</td>
<td>Privacy enhancing technologies</td>
</tr>
<tr>
<td>PKI</td>
<td>Public Key Infrastructure</td>
</tr>
<tr>
<td>PSPs</td>
<td>Private Sector Provisions</td>
</tr>
<tr>
<td>RFID</td>
<td>Radio-Frequency Identification</td>
</tr>
<tr>
<td>TIO</td>
<td>Telecommunications Industry Ombudsman</td>
</tr>
</tbody>
</table>
List of Diagrams and Tables

List of Diagrams

Diagram 7.1.  Industry Code Regulators and Supervisory Authorities. 147
Diagram 8.1.  Investigation and Resolution Process for Breach of NPPs. 159

List of Tables

Table 8.1. Telephone and written enquiries received by the OPC from 2008-10, and the OAIC for 2010. 162
Table 8.2. Written Complaints and Own Motion Investigations (OMIs) closed by the OPC for 2008-10, and the OAIC for 2010-11. 162
Table 8.3. NPP and non NPP related complaints closed without investigation by the OPC for 2008-10, and the OAIC for 2010-11. 163
Table 8.4. NPP related telephone enquiries received by the OPC for 2008-10, and the OAIC for 2010-11. 167
Table 8.5. Privacy complaints received by the TIO for 2008-11. 171
Table 8.6. Privacy complaints investigated by the TIO for 2008-11. 172
Table 8.7 Complaints investigated and closed by the ACMA under the Do Not Call Register Act 2006 (Cth), and Spam Act 2003 (Cth) for 2008-11. 173
Table 8.8. Outcomes after the close of investigations by the OPC for 2008-10, and the OAIC for 2010-11. 188
Table 8.9. Outcomes after the close of investigations by the TIO for 2008-11. 192
Table 8.10. Outcomes after the close of investigations by the ACMA under the E- Marketing Code for 2008-11. 195
Publications Based on this Thesis


Abstract

This thesis is concerned with the impact of information technology on e-commerce users’ right to privacy. It argues that privacy is a human right which cannot be traded off against commercial interests. In this context, the thesis examines whether the current Australian federal statutory privacy protection framework adequately protects the privacy of Australian e-commerce users.

The thesis examines the legal theories that justify privacy as a human right and impose obligations on the State to protect these rights. It compares the Australian approach with the most influential international developments in the European Union (EU) and Organisation for Economic Co-operation and Development (OECD) which may be regarded as establishing international norms of conduct for information privacy. The EU and OECD principles are used as comparators in assessing whether the Australian federal regulatory framework gives adequate recognition to privacy as a human right. The thesis concludes that the Australian federal legislation fails to give adequate protection to the privacy rights of e-commerce users and the approach used in the EU should be used as a model for change.
Chapter 1: Introduction

1.1 Introduction

This thesis examines the impact of information technology on information privacy.\(^1\) It focuses on the threats to e-commerce users by the invasive activities of e-businesses and Internet service providers (ISPs) that collect, use and transfer personal data. If privacy is recognised as a human right it will have priority over commercial interests. This has important implications for the regulation of e-commerce. The proposed amendment to the Preamble to the EU Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (‘Convention 108’) is instructive in this regard. It states:

> Considering that it is necessary, given the diversification and intensification of processing and exchanges of personal data, to guarantee human dignity and the protection of human rights and fundamental freedoms of every person, in particular through the right to control one’s own data and the use made of such data.\(^2\)

As would have been noted, the above statement crystallises the issues surrounding e-commerce users’ rights to privacy in relation to their personal information. This thesis examines how far Australian federal regulation protects an e-commerce user’s rights to privacy. Chapter 1 sets the context for the discussion of e-commerce.

1.2 E-Commerce: the Context

The term ‘e-commerce’ as used here, refers to all commercial transactions conducted over the open networks of the Internet, and wireless communications networks. E-commerce involves both business-to-consumer (B2C) transactions and services, and the services provided by Internet service providers (ISPs) that facilitate e-commerce. These services include the marketing, advertising, sale and distribution of products through the Internet.\(^3\)

---

\(^1\) Information privacy is also referred to as ‘data privacy’. Throughout the thesis the term ‘information privacy’, ‘data privacy’ and ‘privacy’ will be used interchangeably.


Information technology and electronic commerce (e-commerce) has fundamentally transformed the ability to communicate, to access information, and purchase within a global market. The benefit of e-commerce is that the store is effectively open 24 hours a day, 7 days a week. E-commerce offers consumers and businesses greater choice and convenience, increased competition and information on goods and services. Orders can be processed online in real time, or off-line in batch process without any geographical constraints; local shops can compete with national or multinational companies for consumers located anywhere in the world. Products and services offered over the Internet are in a form very close to that of true free market competition without the imposition of political and geographic boundaries. The services and goods provided by e-commerce businesses include all forms of text, sound and image, Electronic Data Interchange (EDI), EFTPOS, electronic banking, digital cash, and other electronic payment systems. Global information services and products account for trillions in revenue as the Internet’s phenomenal global growth has developed cost-effective e-commerce applications.4

1.3 The Issue of Information Privacy for E-commerce Users

The problem for e-commerce users is not just the potential for abuse of individual privacy by small internet businesses but also by huge multinational Internet companies such as ‘Google’,5 ‘Yahoo’, ‘Microsoft’, ‘MySpace’ and ‘Facebook’.6 Information about users is accessed by ISPs and e-businesses with or without users’ consent and knowledge particularly in situations where data mining and surveillance technology is used to collect information from e-commerce users for direct marketing and online advertising. The unauthorised collection, monitoring, use, and sharing (and trading) of e-commerce users’ personal information with organisations not party to the transaction without the knowledge or consent of individuals is prevalent. There has been public backlash following recent media reports of ISPs such as ‘Google’, social networking websites such as ‘Facebook’,

and e-businesses monitoring Internet and e-commerce users with Google admitting to unauthorised data collection. As far back as 1994, an estimated five billion records containing information of every person was held in U.S. computers. It was estimated that by the year 2000 even more personal information would be held in more than 20,000 or so personal databases held by corporations in the U.S. which include financial details, medical information and lifestyle habits and other confidential data. Then, the credit reporting industry itself accounted for 400 million files and these files were further updated with more than two billion entries every month that facilitate 1.5 million credit decisions every day. DoubleClick has agreements with thousands of web sites and maintains cookies over 100 million unique users with each linking to hundreds of bites of information about users’ browsing habits. By 2005, the database company, ChoicePoint had more than 250 terabytes of data regarding the lives of 220 million adults. In 2010, it was reported that the purchasing preferences of some 8 million Australians had been harvested by the world’s largest data exchange. It is also reported that companies such as eBay allows information from its web browsers to be collected and sold through data exchanges. The current rates of data collection are likely to be exponentially higher.

Consumers are worried that companies will take advantage of consumers’ interaction online and invade their privacy to capture information about them for marketing and other

---


8 Fred H Cate, Privacy in the Information Age (Brookings Institution, 1st ed, 1997) 2.


13 Julian Lee, 'Online Tracker Claims to Have Data on 8 Million Australians', Brisbane Times (Brisbane) 6 October 2010 <http://www.brisbanetimes.com.au/technology/technology-news/online-tracker-claims-to-have-data-on-8-million-australians-20101005-1667y.html>. The online behaviour of millions of Australians is tracked and auctioned to advertisers. ‘BlueKai’ the largest data exchange company claims to have data on 8 million Australians.

secondary purposes without their informed consent.\textsuperscript{15} The data may be used by more than one organisation or for multiple purposes. Personal information that is voluntarily provided may be shared without the individual’s consent or misused. Recent research findings in Australia, the United Kingdom (UK), the United States (U.S.), and New Zealand (NZ) show that the level of public concern for privacy and personal information has increased since 2006.\textsuperscript{16} In a study commissioned by the then federal Australian Privacy Commissioner\textsuperscript{17} in 2007, it was found that 50 percent of Australians are more concerned about providing information online than they were in the previous two years.\textsuperscript{18} In an earlier survey conducted by the then Office of the Federal Privacy Commissioner in 2001, respondents were asked about their attitude to unsolicited marketing information from organisations that they had not previously dealt with. The survey results showed that most people were concerned about how their contact details had been obtained, and complained that the organisations should have obtained their permission before sending them marketing material. Twenty one percent of those who took part in the survey complained that it was an invasion of their privacy. Those individuals who wanted to get off the marketing list complained about their inability to do so.\textsuperscript{19} In the survey about 90\% of respondents thought that permission should be obtained prior to sending them marketing information.\textsuperscript{20} Despite a much more protective regime in the EU, there is still considerable

\begin{footnotesize}
\begin{enumerate}
\item[17] It is to be noted that with the passing of the Privacy Amendment (Enhancing Privacy Protection) Bill 2012 introduced on 23 May 2012, the Office of the Privacy Commissioner was integrated into the Office of the Australian Information Commissioner (OAIC) with effect from 1 November 2010. The legislative structure of the Office of the Australian Information Commissioner now includes three statutory office holders. These are: an Information Commissioner; and Freedom of Information Commissioner and the existing Privacy Commissioner. See Office of the Australian Information Commissioner’s Website, ‘Privacy Law Reform’ <http://www.privacy.gov.au/law/reform>; Australian Law Reform Commission, For your Information: Australian Privacy Law and Practice (‘Report 108’) (2008) 1528-29 [46.2]-[46.5].
\item[20] The survey result is from a research commissioned by the Office of the Federal Privacy Commissioner and undertaken by Roy Morgan Research. See Roy Morgan Research, ‘Privacy and the Community’ (July 2001
\end{enumerate}
\end{footnotesize}
concern about control of personal data. A recent survey in Europe also indicates that about a quarter of social network users (26 percent) and online shoppers (18 percent) feel that they are not in complete control over their personal data.\(^{21}\)

Consequently, it is not necessarily the case that the public do not care about infringement of their privacy. This, however, contrasts with the willingness of internet users to voluntarily sacrifice privacy and personal information by agreeing to the provider’s terms and conditions which may seriously compromise the user’s privacy. There is, on the one hand the desire to protect e-commerce users acting against their own best interests by waiving privacy rights and on the other hand requiring users to take responsibility for protecting their own private information.\(^{22}\) Chapter 4 examines this issue.

The problem is in finding an appropriate balance between the benefits of e-commerce against the privacy risks that technology brings. The challenges arise from the use of privacy invasive information technologies by data collectors, (these are outlined in Chapter 2), the complexity of laws, the trans-border flow of information; and the existence of a multiplicity of approaches and operating standards involving the overlapping roles of regulators; and the lack of compliance and enforcement by privacy protection regulation. There is the added difficulty for regulators in making the regulatory framework sufficiently adaptive to respond to very rapid changes in technology.

The problems for information privacy protection arise from the failure to adequately recognise and enforce privacy as a human right by the Australian legislative framework for privacy. The thesis will argue that information privacy protection in Australia needs to be anchored to the recognition that privacy is a fundamental human right not to be traded off against economic interests. The Australian regulatory framework when analysed gives preference to economic interests.

\(^{2001}\) <http://www.roymorgan.com.au>. Refer to Figure 3: Responses to receiving unsolicited marketing information from organisations they have never dealt with before.


\(^{22}\) Kieron O'Hara and Nigel Shadbolt, 'Privacy on the Data Web' (2010) 53(3) Communications of the ACM.
1.4 The Scope and Outline of the Dissertation

The focus of the thesis is on information privacy and not the broader issues of privacy generally. It is concerned with the regulation of private sector organisations and does not consider information privacy in the context of government and public sector agencies. It focuses in particular on the collection of ‘personal information’ or ‘personal data’ through technological devices by the private sector organisations that include online e-commerce businesses and ISPs, operating for commercial purposes over the Internet. It does not discuss social networking sites as the emphasis is on individual e-commerce users.

Chapter 2 examines some of the relevant technologies which affect information privacy and their negative impact. It draws attention to the risks, and harm resulting from the activities of data collectors in the collection, storage and dissemination of personal information and surveillance of data subjects.

The core of the thesis is the erosion of the right to privacy with respect to e-commerce users in Australia. An analysis of the concept of privacy and the protection of privacy as a human right is undertaken in chapter 3. The key argument is that there is a personal human right to privacy which extends to protect information privacy of e-commerce users. The thesis argues that privacy is a fundamental human right and that individuals have a right to privacy against unwanted surveillance, and the collection and use of personal information without their consent.

Chapter 4 examines the role of consent and whether it should be sufficient for the waiver of personal rights to privacy. This is discussed in the context of the current practices of e-commerce providers in relation to privacy policies, bundled consent and the like. The Chapter then considers consent in the context of the contractual model which assumes

---

23 The term ‘personal information’ and ‘personal data’ is used interchangeably and in the meaning assigned to the term ‘personal data’. ‘Personal data’ is defined in Directive 95/46/EC as ‘any information relating to an identifiable natural person’ where an identifiable person is ‘one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, psychological, mental, economic, cultural or social identity.’


25 There is no statutory definition of the term ‘privacy’ and an unqualified right to personal privacy seems unknown. See Williams v Settle (1960) 1 WLR 1072. In Australia the case of Victoria Park Racing and Recreation Grounds Co. Ltd. v Taylor (1937) 58 CLR 479 declares that there is no common law right to privacy per se in Australia. Nevertheless s 51 of the Australian Constitution Act 1901 (Cth) provides for the passing of legislation implementing international declarations, conventions and treaties signed on behalf of Australia, including the Human Rights and Privacy Declaration and Convention.
bargaining between equals. It contrasts this with modern consumer protection legislation which recognises that consumers are not always in an equal bargaining position, that consent is not always sufficient to be contractually bound and provides protection against unfair terms contained in standard form contracts.

Chapter 5 examines the most influential international developments in the EU and OECD in relation to information privacy. It examines the 1980 OECD Guidelines\(^{26}\) and the principal EU Directive protecting privacy, EU Directive 95/46/EC.\(^{27}\) These provisions are especially important in their recognition of privacy as a human right entitled to protection. The importance of this recognition is highlighted through the discussion of the EU Directive and OECD Guidelines. The international experience provides a comparator to the Australian provisions. It is used to highlight in the following chapter the differing approach to the protection of privacy under the Australian legislative provisions and accompanying National Privacy Principles.

Chapter 6 examines the federal legislative framework for privacy protection in Australia.\(^{28}\) Its emphasis is on the legislative approach. It does not deal with the limited developments in the common law for protection of privacy which has little general impact on privacy invasive technologies in e-commerce.\(^{29}\) It considers whether the current information privacy protection framework in Australia provides effective privacy protection to e-commerce users. It examines the limits of the Privacy Act 1988 (Cth) and whether it meets the EU’s standard in providing effective and adequate information privacy protection. It also examines the inconsistencies and gaps between the Privacy Act 1988 (Cth) with those under the Telecommunications Act 1997 (Cth); the Spam Act 2003 (Cth) and Do Not Call Register Act 2006 (Cth). It will where relevant illustrate the limitations of the Australian statutory privacy framework in the light of some features of comparative protection in the UK, the U.S., and NZ. This provides insights into how regulators in other jurisdictions and in Australia resolve the issues of information privacy and data security.

An important aspect of information privacy protection is compliance and enforcement of the National Privacy Principles (NPPs). Chapter 6 provides a detailed examination of the

---

\(^{26}\) An extract of the OECD Guidelines is provided in Appendix 1.

\(^{27}\) See Directive 95/46/EC in Appendix 2.

\(^{28}\) It does not consider state legislation which may impinge on privacy issues.

\(^{29}\) Nor does it consider recent debates upon whether there should be a statutory tort of privacy. Refer to the discussion on the limited scope of the common law in chapter 6 [1].
NPPs which provide guidelines in relation to the collection, use, disclosure, access and correction and transfer of personal information. It examines whether the implementation of the standards set for information handling have in reality improved privacy protection, and the control that people have over the use of their personal information for example in preventing data mining, behavioural advertising, direct marketing, and the trans-border flow of personal information; and whether the current framework comply with information protection framework for trans-border flow of information. Since the NPPs do not apply where there are comparable industry codes or codes under other legislation, chapter 7 deals with regulation and industry codes under the Telecommunications Act 1997 (Cth) and the Spam Act 2003 (Cth).

Chapter 7 examines industry regulation under sector specific legislation as well as selected industry codes of practice/conduct. It examines two sector specific industry codes that adopt privacy codes that are permitted and approved under the Privacy Act 1988 (Cth). It also considers the problem of overlapping roles and powers of industry regulators and code authorities established under specific legislation and the difficulties this causes in implementing coherent privacy legislation.

Chapter 8 explores the question of compliance with, and enforcement of the current legislative framework, the NPPs, and specific industry Codes of Practice related to e-commerce. It discusses whether industry regulation and codes of practices have been effective in providing information privacy protection. It examines the problems for regulators in providing information privacy protection as well as the limitations of industry regulation for e-commerce users in Australia. The role and power of regulators and code authorities in relation to compliance, complaints handling, enforcement, and what remedies and sanctions there is for breach of privacy is examined in this chapter.

The concluding chapter summarises the findings of this thesis and discusses what more needs to be done for more adequate and effective information privacy and data security for e-commerce users. It assesses the current level of protection for information privacy, examines the legislative proposals for reforming the Australian information privacy framework, and finally makes recommendations for reform.
Chapter 2: Information Technology and How Privacy is Violated

2.1 Introduction

This chapter examines how data collectors engaged in handling personal information invade the privacy of e-commerce users through use of techniques such as data mining\(^1\) and surveillance technology. Through use of such technology, information gatherers are able to harvest personal information of ecommerce users and use it without their consent or knowledge.

An organisation may collect details such as the customer's name, postal and e-mail addresses, credit card details etc., for an e-commerce transaction. But data collection extends well beyond this to consumer information obtained from websites when users’ access search engines, or use the Internet for e-commerce transactions. The online activities of e-commerce users are constantly monitored using electronic surveillance devices. Besides collecting information using data surveillance technology, information is also collected indirectly from other sources such as when a private sector organisation buys a list, or has access to information from another database, or when an individual gives information about a third party to an organisation for example during market research, or for life insurance purposes, or where a contractor collects information from an organisation to carry out its obligations under a contract. There is a market for information as a traded commodity which generates huge profits for data collectors.\(^2\) So it is not surprising that

---

\(^1\) Data mining is the extraction of hidden predictive information from large databases using technologies that can be implemented rapidly on existing software and hardware platforms to enhance the value of existing information resources. Data mining technologies can be integrated with new products and systems as they are brought on-line. See Kurt Thearling, An Introduction to Data Mining: Discovering Hidden Value in Your Data Warehouse, (online) (undated) (Accessed on 20 December 2012) <http://www.thearling.com/text/dmwhite/dmwhite.htm>.

many database companies sell information about users or provide lists of their customers’ e-mail addresses to other direct marketing companies.\(^3\) Two prominent websites ‘Google’ and ‘Facebook’ have been monitoring and collecting personal information for secondary use without users’ knowledge, or explicit consent.\(^4\) The information collected included passwords and emails.\(^5\) Google is alleged to have tracked users on more than 1 million websites that display its advertisements. The Canadian privacy watchdog accused Google of collecting complete emails and accused Google of violating the privacy of thousands of Canadians.\(^6\) Other data exchange companies such as ‘BlueKai’, a California based company, and ‘Phorm’ (a British company) are involved in tracking online users without notification of data collection, or notification that such information will be used for secondary purposes or shared with third parties. They have been able to access personal information posted on websites by users. This is illustrative of the huge risks of invasion of personal privacy. Where there is covert collection of personal information, the consumer may have no knowledge of the information collection, who the data collector is, or if their consent to the use of their personal information has been obtained. This has serious implications for protection of e-commerce user’s rights to privacy.

The discussion following examines the technology used for information gathering, and examines some common applications of technology in data analysis such as behavioural advertising, consumer profiling, creation of digital dossiers, sentiment analysis, and their impact on privacy.

---

\(^3\) Electronic Privacy Information Centre (EPIC), Cookies (epic.org, 2011) [http://www.epic.org/privacy/internet/cookies/].


2.2 Privacy Invasive Technologies

2.2.1 Cookies and Related Technologies

‘Cookies’ and ‘web bugs’ are key features that allow data collection.7 ‘Cookies’ are electronic bugs which attach to the information system and track internet users’ activities.8 It attaches to server side connections (such as CGI scripts) to both store and retrieve information on the client side of the connection. Cookies need to be enabled in a user’s Internet browser and are especially helpful if the user uses the same computer and browser. The user may save search settings such as Google searches, and location without having to make a new search every time the user logs on to the same computer and browser. ‘Cookies’ allow access to information that is stored online9 about purchases and detailed records of customer preferences. For example when a web user requests a page from a web site the request is sent via the user’s browser and answered by a program known as a ‘server’; upon receiving the request for a page the server sends back the requested page as well as an instruction to the browser to set or write a ‘cookie’ into the user’s computer storage.10 The web browser complies with this instruction and each time a user requests a web page the web browser checks for ‘cookies’ in the user’s computer. If there is such a cookie the browser transmits a record of the activities of the user together with the request for the web page to the web server at the same time. A ‘cookie’ can follow a user wherever the user goes. The Web site that stored the original data can access it and the individual cannot share any ‘cookie’ information between different Web sites.11

A web bug is an electronic tag that is similar to a cookie. Web bugs are designed to monitor who is reading the web page or e-mail message and are considered to be similar to an Orwellian Big Browser.12 Web bugs are often invisible because they are typically only 1-by-1 pixel in size and have a function similar to cookies and sometimes known as ‘single

---

8 Electronic Privacy Information Centre (EPIC), above n 3.
9 Senate Select Committee on Information Technologies, above n 7.
pixel GIFs'. Web bugs may be written into the code of a web page or of html-enabled e-mail messages. Whenever the user visits a page or message, the web server from which the web bug comes identifies information such as the Internet Protocol (IP) address of the computer that fetched the web bug; the Uniform Resource Locater (URL) (i.e. the address) of the page that the web bug is located on; the URL of the web bug image itself; the time the web bug is viewed; the type of browser that fetched the web bug image; and if there is a cookie that has been set previously by the same company that has set the web bug.14

There are a variety of other applications which may compromise privacy. Web 2.0 is associated with web applications that facilitate interactive information sharing, interoperability, user centred design and collaboration on the World Wide Web.15 A Web 2.0 site allows its users to interact with others and to change website content. Hosted services, social networking web sites, blogs and video sharing web sites such as ‘FaceBook’, ‘Bebo’, ‘MySpace’, and ‘U -Tube’ use Web 2.0. Personal details stored by these organisations may be used for commercial purposes.16 Those web sites that do not use Web 2.0 are non-interactive and e-commerce users are limited to passive viewing of information that is provided to them.17

The Hypertext Transfer Protocol (HTTP) protocol is a technology that enables web pages to be transported between users and a web server.18 The HTTP protocol functions similarly as the Web 2.0 in that it sends the web server information every time a user requests a web page from the web site without the knowledge of the user. The information sent may vary depending on the options set in the user’s web browser and the software programs used by the web site. The information collected by the HTTP protocol includes the user’s domain name and location, the address on the web page that the user requester the information

13 Senate Select Committee on Information Technologies, above n 7, 19.
14 Ibid.
16 Australian Broadcasting Corporation, 'Facebook Admits Privacy Breach' ABC News (online) 19 October 2010 <http://www.abc.net.au/news/2010-10-19/facebook-admits-privacy-breach/2303858>. Facebook’ has admitted to providing access to ‘Facebook’ members’ names and, in some cases, their friends' names, to companies that build detailed databases on people in order to track them online.
18 Senate Select Committee on Information Technologies, above n 7.
from, the search query keyed into the search engine, the user’s e-mail address, and
information about the software and hardware being used.\textsuperscript{19}

Most of the privacy invasive applications depend upon this technology. There are other
new surveillance technologies such as Caller ID, Global Positioning System (GPS)
satellite tracking, to biometric scans which can easily track and identify individuals. These
technologies can pinpoint an individual’s exact movements and activities anywhere in the
world.\textsuperscript{20}

Malicious software (malware)\textsuperscript{21} facilitates the tracking of an individual’s transactional
information, user preferences and user activity in cyberspace.\textsuperscript{22} Malware programming
(code, active content, and other software) is designed to disrupt or deny operation, gain
unauthorised access to system resources, gather information that leads to privacy loss or
other abusive behaviour. Examples of malware include ‘spyware’, ‘Trojan horses’,
‘viruses’, ‘web bugs’, and ‘worms’.\textsuperscript{23} The thesis will focus on cookies which are the most
commonly used technology for data collection on the Internet.\textsuperscript{24} Data surveillance utilises
this form of technology to collect information about e-commerce users without their
consent.\textsuperscript{25}

\textsuperscript{19} Senate Select Committee on Information Technologies, above n 7, 20-21.
\textsuperscript{20} Science and Technology Options Assessment (STOA), ‘Project No: IV/STOA/RSCH/LP/politicon’ (Report
commissioned by the Civil Liberties Committee, European Parliament, 1997)
\texttt{<http://www.europal.europa.eu/committees/libe_home.en.htm>}. The report states that current information
technology is able to track the activities of individuals; These technologies are also being used by
governments to track activities of dissidents, human rights activists, journalists, student leaders, minorities,
trade union leaders and political opponents; See also David Banisar and Simon Davies, ‘Privacy and Human
\texttt{<http://gilc.org/privacy/survey/intro.html>}.\textsuperscript{21}

\textsuperscript{21} Troy Nash, ‘An Undirected Attack Against Critical Infrastructure: A Case Study for Improving Your
\texttt{<http://211.167.103.140:82/1Q2W3E4R5T6Y7U8I9O0P1Z2X3C4V5B/www.us-
cert.gov/control_systems/pdf/undirected_attack0905.pdf>}.\textsuperscript{22}

\textsuperscript{22} Senate Select Committee on Information Technologies, above n 7; Electronic Privacy Information Centre
(EPIC), above n 3.

\textsuperscript{23} Troy Nash, above n 21.

\textsuperscript{24} Senate Select Committee on Information Technologies, above n 7.; See also European Commission,
processing of personal data and the protection of privacy in the electronic communication sector’ for further
discussion on the implications of ‘cookies’. Directive 2002/58/EC is currently under review. See also
and Enforcement, and More to Come’ (EDPS/09/13, The European Guardian of Personal Data Protection

2.2.2 Dataveillance/data Mining

Data surveillance involves collecting information about a person by monitoring that person’s activities, and recording information using surveillance technology. Data mining and surveillance over the Internet is referred to as ‘dataveillance’. Dataveillance is the systematic use of personal data systems in the investigation and monitoring of the actions or communications of one or more people. Dataveillance is usually surreptitious with information collected without the knowledge or consent of the e-commerce user. Clarke explains that ‘dataveillance is computer based with watch and report’ responsibility delegated to a reliable, ever wakeful servant’ such as a ‘cookie’. Dataveillance is a cost effective method of mass surveillance of individuals and groups.

Two examples of new data surveillance/data mining technologies are: firstly the RFID chip (Radio-Frequency Identification) when embedded into objects enables communication between an individual and a device, and a device to a device, or a device to a grid; secondly ‘behaviour-tracking ad system’ that which has been launched by Internet service providers (ISPs) to bring Internet users more relevant advertising and to benefit e-commerce businesses. As noted earlier, the emphasis in the thesis will be on cookies rather than newer forms of surveillance just mentioned.

Many e-commerce businesses and online retail merchants use some form of dataveillance/data mining technology such as behaviour-tracking ad systems which

---

28 Ibid.
29 Dataveillance employs data mining technology utilising cookies for the indiscriminate collection of digital information as is passes through internet networks. It is scrambled and meaningless until processed. It involves the use of sophisticated data analysis tools to discover information that is previously unknown, new patterns, and relationships in large data sets. The tools used for data mining may include statistical models, mathematical algorithms, and machine learning methods (algorithms that improve their performance automatically through experience, such as neural networks or decision trees. Data mining algorithms have been likened to an excavator which excavates and sifts through large amounts of information. Data mining is a valuable tool for businesses as it provides efficient discovery of valuable, non-obvious information from a large collection of data such as purchasing habits, preferences, and the prediction of consumer behaviour. See Maureen Cooney, 'Report to Congress on the Impact of Data Mining Technologies on Privacy and Civil Liberties, DHS Privacy Office Response to House Report 108-774' (US Homeland Security, 6 July 2006); Jeffrey W. Seifert, 'Data Mining: An Overview' Congressional Research Service and The Library of Congress, (7 June 2005 2005) <http://fpmall.info/hosted_resources/crs/RL31798_050607.pdf> 1; Marx G T and Reichman N, 'Routinising the Discovery of Secrets' (1984) 27(4) Behavioural Scientist 423, as cited in Roger Clarke,above n 26, 501.
30 The thesis will not be discussing other surveillance technologies as caller ID, GPA tracking; maybe as a footnote to the Cookies and related technologies.
employ cookies to monitor potential customers. In the process, personal information about the website visitor may also be collected. For example ISPs, e-business companies that specialise in data mining collect e-mail addresses from sources that include messages posted on social networking websites, e-mail lists, news groups, or domain name registration data. The information collected by cookies includes details such as the frequency of visits to a website the visitor makes, the nature of the searches the visitor makes, the users behavioural patterns, such as, the visitor’s dislikes and preferences in terms of brand choice, affordability, the type of credit card used, credit cards details, e-mail addresses etc. These types of information provide valuable competitive advantage to businesses. The information collected is later processed to allow the ISPs or businesses to target specific Internet users. Previously-gathered information can be analysed, and used.

2.2.3 Applications

E-businesses track consumers over time and build up data on consumer interests and shopping activities. The aggregation of data involves combining the information collected from e-commerce users or Internet users. Data banks or data ‘silos’ process information collected using data mining technology that tracks every click an Internet user makes. The data that is collected may be combined in a number of ways which might otherwise not be practicable. Database companies are able to correlate and manipulate the data collected

31 Besides Behaviour-tracking ad system, Radio Frequency Identification (RFID) tags are another form of data collection technology used in information and communications technology systems to support intelligence gathering facilitate and the control and tracking of personal data. The use of RFID technology makes it possible to identify the owner of the RFID tags. The Joint Research Centre (JRC) found that the use of RFID tags in information and communications technology systems create opportunities for access to private information by third parties for commercial purposes. The JRC proposed that the use of RFID tag be regulated by legislation addressing identity related issues.

32 Roger Clarke, above n 26.


34 ‘Facebook’ has admitted to providing access to ‘Facebook’ members' names and, in some cases, their friends' names, to companies that build detailed databases on people in order to track them online. See Australian Broadcasting Corporation, above n 16.

through the process of data matching, ‘sentiment analysis’, customer profiling, and the creation of digital dossiers.36

‘Sentiment analysis’ involves analysis of online conversations which are mined for words and thoughts to be used for a commercial advantage.37 Internet websites such as ‘MySpace’ and ‘Facebook’ collect information that users provide such as where you live, your conversations with friends and family on social media websites, and what your preferences are to be used for sentiment analysis.38 The information about customer’s preferences, purchase, and transactions details are collected and stored in databases for future use.

Profiling refers to the process of construction and application of computerised profiling technologies. Both individuals and groups of individuals may be profiled. Profiling allows one to discover patterns or correlations in large quantities of data, generated in a database. Profiling makes a judgement about a particular individual based on past behaviour of other individuals who appear to be statistically similar and stereotyping individuals.

Profiling is not restricted to retrospective investigation. Profiling can be used for example in the case of credit scoring, price discrimination, or identification of security risks.39 Profiles are also used by advertisers and direct marketing companies to predict user’s preferences, interests, and possible future purchases. For e-businesses, customer profiles and detailed records about purchasing preferences provide a valuable competitive edge and are a major currency in e-commerce.40 Profiling users based on their preferences and habits helps e-businesses and other data collectors to plan strategies and market their products to specific target groups and individuals twenty four hours a day seven days a week.

36 Roger Clarke, above n 26, 501; Colin Bennett, Regulating Privacy: Data Protection and Public Policy in Europe and the United States (Cornell University Press, 1992) 19.
39 Mireille Hildebrandt and Serge Gutwirth (eds), Profiling the European Citizen: Cross Disciplinary Perspectives (Springer, 2008) 303-343.
40 Ibid.
The increasing interconnectedness, affordable, fast, on-line systems enable the building of digital dossiers. Digital dossiers can be assembled from information about a person by accessing personal details aggregated by banks, businesses, websites, employers, ISPs, and other entities. Digital dossiers provide information that can be likened to an individual’s curriculum vitae. Digital dossiers about an individual’s status, reputation and credibility and can be used to determine eligibility and suitability for jobs, and credit worthiness.

The processed data in the form of profiles and digital dossiers can be disseminated or can be made accessible easily; it can be transferred quickly from one information system or database to another and across borders without the knowledge or consent of the data subject.

The underlying issue related to profiling and the creation of digital dossiers is the violation of privacy and indiscriminate profiling of individuals and groups and the compilation of information about a person randomly collected from cyberspace to create a digital dossier. Individuals and groups more often than not do not know that they are being profiled or a digital dossier is being compiled about them. Not knowing that a profile or digital dossier has been created on them makes it impossible for individuals and groups to object to the creation of profiles or the way that their profile is being used, the basis on which a benefit is withheld, and the way they are being treated. Profiling an individual, or group can stigmatise and create risks for individuals. For example, a group profile may describe specific behaviours or other characteristics of a category of people such as age, ethnicity, health risks, earning capacity, morality rates, credit risks etc.

Internet users may make users susceptible to discriminatory business practices such as placing a difficult customer last on a priority queue or simply not dealing with them at all.

---

42 Ibid.
43 Ibid.
Profiles also expose e-commerce users to risks of the information being linked to other information such as names, addresses and e-mail addresses making them personally identifiable. There is a risk that profiles may end up with those who are not entitled to access or use them and raise concerns about data security breaches and identity theft. This raises issues of data security to which we now turn.

2.3 Data Security

Online privacy for consumers is seriously compromised by data security breaches. Personal data is at risk of unauthorised access, falling into the wrong hands, misused or becoming a commodity for illegal sale; it is easy to find a service on the internet that sells information about people’s bank accounts, the amount of money in them and credit card numbers.\(^{47}\) This exposes individuals to identity theft, loss of reputation, confidentiality and potential loss of valuable intellectual property rights. Insecure systems can give rise to identity fraud if a party acquires a user’s identifiers and in particular identity authenticators.\(^{48}\) Examples of identifiers include usernames, password, personal identity number (PIN), pass phrase, private signing keys (identity authenticators), credit card details, the billing address, and the expiry date. It can lead to the initiation of transactions by someone other than an authorised user of the device. When a user transfers funds to someone’s account or make a payment for goods and services provided for someone else then there is a record of previous transactions in a log file.

It is obvious that unless appropriate measures are taken the e-commerce user’s personal data is at risk of being compromised. The problem is not necessarily that appropriate technology has not been used to protect digital information, it might be, for example, organizations provide access to their record systems over the phone to anybody in possession of a few easy-to-find pieces of personal information such as birth dates, and mothers’ maiden names etc.\(^{49}\) There are many ways in which the integrity of information may be violated with or without malicious intent. For example when an employee either


\(^{49}\) Ibid.
accidentally or maliciously transfers a data file, or when a computer virus infects a computer, or when an unauthorised user vandalises a web site.

Data insecurity may also arise from the vulnerabilities and weaknesses in the data system that may cause harm to informational assets. For example risks may be inherent in software, including Web browsers, plug-ins, and active content applications such as Java applets and ActiveX controls.\(^50\) There may also be weaknesses in the generic nature of the architecture and within which the components are placed which are lacking comprehensive security strategy.\(^51\) For example the active content that is embedded in the Web pages everywhere may overcome the limitations of Hyper Text Mark-up Language (HTML). There is the capacity to access personal files, corrupt files or send data back over network connections, or deposit computer viruses without users’ knowledge.\(^52\) Similarly wireless, specifically in GSM (Global Standard Mobile), are subject to risks through gateway vulnerability and the ‘man in the middle’ attack (the latter occurs as cellular towers do not authenticate users of cellular phones).\(^53\) If not secured the data transfer process can easily be intercepted, as a result of which e-commerce providers have the responsibility to take additional steps to ensure the security of their transactions.

There is the risk of misuse of stored data by employees, and unauthorised access when individuals hack into databases.\(^54\) Stored data may be leaked or accessed by unauthorised parties\(^55\) with evidence of increased occurrence.\(^56\) There may also be interference with transactions undertaken by an authorised user including diversion of a legitimate payment to another account and the diversion of the delivery-point of goods and services for which an order is placed.

---


51 Ibid.

52 Anup K Ghosh, above n 35, xiii.


56 Australian Securities and Investments Commission (ASIC) warned consumers of the pitfalls and scams to avoid and for consumers to call and to report instances of scams to its FIDO website. For further details see Australian Securities and Investments Commission, Fraudulent Emails and ‘Phishing’ Attacks, Watch Out-Some Emails Look Surprisingly Genuine’ (online) (2007) <http://www.fido.asic.gov.au/fido>
There are numerous media reports of breach of data security and sale of personal information for commercial interests.\(^57\) The Privacy Rights Clearing House, a non-profit consumer group in the U.S. reports that more than a half a million records have been compromised since 2005. In Australia, the Australian Payments Clearing Association report that the value of online credit card fraud in Australia exceeded $102 million during the period 30 June 2009 – 31 July 2010.\(^58\) The largest data security breach involved theft of more than 45 million credit and debit card numbers from TJX companies located in the US, Canada, and possibly in the UK and Ireland.\(^59\) Identity theft is becoming increasingly common and is for example the fastest growing crime.\(^60\) Between the years 2001 – 2002 incidents of identity theft rose 88% according to the Federal Trade Commission (FTC) and the FTC estimated that ‘almost 10 million Americans discovered that they were the victim of some form of ID Theft.’\(^61\) In NZ there were about 900 cases of identity fraud uncovered during the first six months of 2008.\(^62\)

Currently there is no requirement in Australia that e-commerce users be notified when there is a security breach consequently e-commerce users are not in a position take timely action to limit risks to their personal information from risk by for example changing their pin number and passwords.\(^63\) Many forms of data security measures may be taken to

protect by e-commerce users themselves such as the use of privacy enhancing technologies (PET). This is examined in the next section. The obligation of data collectors to provide effective security to protect personal information of e-commerce users is discussed below at [2.3.1.1].

2.3.1 Data Security Technologies

2.3.1.1 Data Collector’s Responsibilities

The security of e-commerce is dependent on the availability of encryption techniques. A secure website uses encryption technology to transfer information from the consumer’s computer to the online merchant’s computer. Encryption encodes data so that even if a computer or network is compromised the data content will be inaccessible to anyone who does not hold the key. Data is encrypted using the recipient’s public key. In the online environment the public keys are used to encrypt and decrypt text. The sender of the message encrypts data using a private key and data can only be recovered by using the sender’s public key. The use of encryption ensures that only the recipient can read it thus ensuring the privacy and security of messages between persons. Information that has been encrypted can be transformed back to its original form by an authorised user who holds a cryptographic key. Only people with legitimate access privileges are able to unscramble the information. Cryptography provides for improved authentication methods, message digests, non-repudiation, and encrypted network communications. Digital signature is the second mode in which cryptography operates. Digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or document.

---

67 Senate Select Committee on Information Technologies, above n 7; See also Roger Clarke, ‘Privacy Requirements of Public Key Infrastructure’ (Paper presented at the IIR IT Security Conference, Canberra, 14 March 2000).
Secure payment gateway systems such as e-Path and PayPal are claimed to provide a unique, powerful and secure system that is the forefront of secure online e-commerce. E-path and PayPal secure payment gateway systems are used to make and accept payments online to e-businesses. E-businesses integrate the e-Path and PayPal secure payment system before it collects customer details and accepts credit card details for online payments. The e-Path and PayPal system will send the information directly to the e-business or redirect a customer to the e-businesses secure e-Path or PayPal payment page to make payment. So that use of secure payment systems reduces one of the key risks of online purchasing.

2.3.1.2 Consumer security devices - Privacy enhancing technologies (PETs)

E-commerce users themselves can take measures to protecting personal information from being accessed or falling into the wrong hands, misused and causing harmed to the data subject through the electronic management of information by using encryption. For example e-commerce users can take a number of measures to disable or circumvent potential privacy invasive technologies such as ‘cookies’, ‘web bugs’ etc. These consumer security devices is collectively called privacy enhancing technologies (PETs). Consumer security devices provide users with the capacity to participate in transactions with adjacent and remote applications and may be used as a standalone device and as a single user device.

Cookie management software helps the user to delete cookies and other persistent identifiers. The Platform for Privacy Preferences (P3P) is an Internet protocol developed by the World Wide Web Consortium (W3C) that allows a user to set preferences in relation to his or her own privacy on the Internet. The user will be able to establish what information they are willing to part with, and what information they are willing to provide.

---

72 Senate Select Committee on Information Technologies, above n 7.
73 Senate Select Committee on Information Technologies, above n 7, 32.
74 Roger Clarke and Alana Maurushat, above n 50.
75 Senate Select Committee on Information Technologies, above n 7, 32.
For example, if a web site’s information practices differ from those specifications the user’s browser may either negotiate with the site on the user’s behalf or it may notify the user of the mismatch. The user may then make an informed decision to consent to the use of the data, attempt manual negotiation or withdraw from further interaction with the site. This, of course, assumes knowledgeable consumers.

An anonymiser is a service that conceals the identity and location of a user’s online computer activity. The anonymiser service is also used in communications so that e-mail address of the sender is not revealed. In a standard connection to a web site, the user’s browser will transmit its Internet Protocol or IP address to the web server so that the server knows where on the network to send the information requested. The IP address can be used to identify the ISP or the organisation through which the user gets access to the Internet. If the user’s personal computer is also an Internet host with its own IP address it can identify the person making the connection to the web site. Anonymisers are designed to break the link between a user’s online interactions and the user itself. An anonymiser service automatically strips identifying information from the message from Web and email traffic and replaces it with more or less random identifiers prior to sending the message to the intended recipient. By connecting to a web anonymiser a user can conceal their identity and prevent the user’s location on the network to be easily traced. The reasons why e-commerce users do not employ these technologies are referred to below.

‘Infomediaries’ are web sites such as Lumeria or Privaseek that gather and organise large volumes of data and act as intermediary between those that want the information and those who supply the information. Infomediaries that allow the user to establish different identities of a single personae; a user can establish sets of rules under which an individual user is able to control the types of information about themselves from being disclosed in the context of identity management and addresses surveillance. Consumer use of infomediaries is referred to below.

77 Senate Select Committee on Information Technologies, above n 7.
79 Senate Select Committee on Information Technologies, above n 7, 22.
Consumer orientated privacy enhancing technologies are relevant only if they are incorporated into everyday practice. PETs are complex to operate and have not been widely adopted by individual users for a number of reasons.  

Firstly to set up PETs, there needs to be an infrastructure that is able to distribute cryptographic keys. Although encryption is an option for protection of transactions and communications there are problems with its use. The infrastructure that supports the general operation of public key cryptography is called Public Key Infrastructure (PKI). Developing standards and legislation is a major focus of government online privacy and these areas are complex issues. Some countries have opposed the use of encryption for non-financial activities. Governments have an interest in being able to freely access digital information for national security and law enforcement. For these reasons encryption software is subject to government regulation. While some countries have banned encryption altogether, countries such as the United States government tried to impose a ban on all secure financial transactions (SSL) with encryption higher than what they could decrypt.

Secondly although it is expected that consumers will take benefit from the assortment of opportunities created by net-enables commerce there is a lack of understanding about critical facts that drive consumer adoption of PETs. While some computer savvy users have been able to employ these technologies, it is not in general public use. Many users are not sufficiently aware of the risks or understand the technical features of software. Most do not carefully read the software licenses or sufficiently understand the security alerts. Consumers may choose to continue a transaction rather than be precluded from conducting

---

82 Senate Select Committee on Information Technologies, above n 7, 28.
84 For example, the Computer Misuse Act 1996 (Singapore) passed by the Singapore government, authorises Singapore’s security services to intercept email messages, decrypt encoded messages and confiscate computers without a warrant in the course of investigations. Similarly, Britain introduced the Regulation of Investigatory Powers Act (RIP) 2000 that made no provisions prescribing for encryption of information but required users to surrender passwords when asked to do so by investigators or face 6 months imprisonment for failing to do so. There is uncertainty about how to ensure the security of private keys and the process of key generation and so on. If the users’ private key is lost or compromised the certification authorities need to be able to revoke certificates. To revoke certificates the certification authority would have to publish a list of revoked certificates. This raise privacy concerns as well as concerns about policies for the generation, storage and back-up of private keys. See Roger Clarke, 'Privacy Implications of Digital Signatures' Xamax Consultancy Pty Ltd (1997) <http://www.rogerclarke.com/DV/DigSig.html >.
85 Senate Select Committee on Information Technologies, above n 7.
transactions on websites that depend on insecure features of web-browsers. Overall cookie management software only provides limited protection in relation to ‘cookies’, Javascript, Java and ActiveX. Cookies and Web bugs may be difficult to detect. Cookies may be blocked or managed but the software varies, is difficult to understand and may be inadequate. A Java can be turned off but it is a complex programming language and without which some web sites will not function.

There are a number of concerns to the P3P protocol these are firstly that users are required to have a level of technical expertise to configure their browsers to individual preferences; secondly P3P protocols assume that users have a minimum amount of information that they are willing to share; and thirdly there is a lack of enforcement capability within the protocol. The P3P protocol is ineffective in ensuring that web sites give and accurate account of their information practices and that user preferences will be respected. It relies on external enforcement provisions for example international and national framework to control deceptive practices. The P3P protocol is still developing and not commercially available.

Some consumers may prefer to use informediaries and react more favourably to the services offered by infomediaries. Individuals using infomediaries encounter problems with using persistent and viable pseudonyms through the open internet protocols to use cryptography. For example individuals are required to manage their online identity and it is not always clear why or to what end one would choose one persona over another in any online context. Individuals using pseudonyms to create an internet identity may need to use multiple identities for different transactions in order to prevent tracking. Keeping track of the different pseudonyms or identities used can be a problem. It is most likely that people may forget what identity they had used for which transaction and which the password they used.

2.4 Conclusion

This Chapter has provided a brief overview of the relevant technology which allows data collection of personal details of e-commerce users. On the one hand there are technologies

86 Senate Select Committee on Information Technologies, above n 7; Roger Clarke and Alana Maurushat, above n 50.
87 Senate Select Committee on Information Technologies, above n 7.
88 Ibid.
89 Jai-Yeol Son, Sung S Kim and Frederick J Riggins, above n 80, 496.
such as cookies, Web 2.0 and Hypertext Transfer Protocol (HTTP) protocol which are essential for the ordinary operation of e-commerce. The benefits both to the consumer and to the provider are obvious. But, new and emerging technologies such as spyware, worms, viruses, and web bugs, the wider use of cookie technology and data analysis has the potential to infringe an e-commerce user’s privacy. Online e-commerce business service providers, ISPs, and social networking websites are currently the primary collectors and abusers of personal information. As outlined in this chapter, there are significant risks to privacy through these technologies. Some of these risks might be counteracted by savvy users utilising privacy enhancing technologies (PET). But for the majority of users, the beneficial protective technology would rarely be utilised. Data collectors could design information systems that may assist in minimising the collection of unnecessary personal information.90

Although PETs play an important role in privacy and data protection, both the European Commission (EC), and the Australian Law Reform Commission (ALRC) support the view that PETs cannot replace legislative and regulatory framework for protecting privacy.91 The onus should be on the data collector to ensure that stored data is secure against unauthorised use, access or theft. It is necessary to ensure that organisations employ adequate precautions to protect data from loss, misuse, unauthorised access, disclosure, alteration and destruction. Abuses are likely to emerge where regulation fails to adequately protect e-commerce users against the wrongful use and disclosure of personal information.92

The next chapter examines what is privacy, the right to privacy as a human right; and why it is important to protect the personal information of individuals.

92 Daniel J Solove, above n 25, 477.
Chapter 3: Privacy

3.1 Introduction

Chapter 2 highlighted the pervasive impact of the activities of data collectors on e-commerce user’s privacy. As noted therein, when e-commerce users purchase online, their activities can be tracked and the information mined to create digital dossiers which can be used and sold for the commercial advantage by data miners and collectors. The person’s life, habits, interests, connections and preferences are both exposed and exploited for financial advantage. This chapter examines whether an e-commerce user can be said to have a ‘right’ to privacy in relation to their personal information, and in this context whether the right is capable of being traded off against commercial interests or qualifies as an inviolable human right which takes priority over other interests.

An individual’s ability to control disclosure of information about themselves is important for the protection of personal interests such as personal integrity, reputation, human dignity, expectations, autonomy and self-determination, happiness and freedom. Implicit in all of this is the individual’s ability to control the flow of information and its accessibility to others by the individual consenting to, making decisions over, and the exercise of the individual’s choice whether to allow or disallow others into the individual’s private space and information. Control over information is connected to how individuals want to be seen, to whom they want to be seen, and in what context. A threat to privacy will be a threat to the integrity of a person and it is the right of each individual to protect his or her integrity and reputation by exercising control over information about them which reflects and affects their personality. The disclosure of those facts that are considered personal and intimate exposes and reveals an individual’s vulnerability and psychological processes that are necessarily part of what it is to be human. Those personality interests

2 So information that a person had purchased Viagra, weight loss treatments, books on child abuse, divorce and country living would reveal a great deal about the individual.
4 Kent Greenawalt, 'Privacy and its Legal Protections' (1974) 2 Hastings Centre Studies 45; See also Beate Rossler, above n 3, 116.
5 Charles Fried, 'Privacy' (1968) 77 Yale Law Journal 75.
6 The duality of the concept of the right to privacy is both a part and a protection for individual personality is more fully discussed by Samuel Warren and Louis Brandeis, 'The Right to Privacy' (1890) 4(193) Harvard Law Review, 194.
can be seriously compromised if the e-commerce user cannot control the disclosure or use of personal information in cyberspace.\textsuperscript{7}

The e-commerce user has been described as having virtual personhood, where information provides links between real-space identity and a virtual person where this information can detrimentally impact reputation and individual identity. However the fact that e-commerce users may value privacy as protecting individual dignity, autonomy, reputation and their ability to control access to information and their relationships with others, may not in itself justify an automatic entitlement to those protections as the community may have a greater interest in requiring individuals to disclose at least some aspects of such information to serve the public good. Stated differently, the difficulty is in striking an appropriate balance between the e-commerce users’ right to privacy in relation to some or all of their personal information on the one hand, and the right of the government and the public to know and to have access to user private information. The chapter examines whether an e-commerce user can be said to have a human right to privacy.

The chapter proceeds as follows. First it discusses ‘what is privacy’. Secondly, it places the issue in the context of an e-commerce user’s privacy. Thirdly, it considers whether there is a Right to Privacy per se in the sense of an inviolate human right. Finally, it considers the right of the State to make inroads into these rights, and more particularly to cede these rights to individuals and agencies of the State to do so. The discussion in this chapter provides the foundations for the chapters following which considers the EU and OECD principles in establishing norms of conduct for protecting privacy.

### 3.2 Privacy

There is a vast volume of literature on the meaning and importance of privacy.\textsuperscript{8} Much of the discussion of what privacy begins with the ground breaking work of Warren and Brandeis in 1890 in United States advocating a tort of invasion of privacy, a ‘right to be let alone’, grounded not on property rights but on the principle derived from German Law of


‘inviolate personality’. What was important was not simply a matter of appropriation of interests but ‘the peace of mind or the relief afforded by the ability to prevent...publication at all’. The later work of Prosser viewed breaches of privacy as comprising four separate torts: invasion of seclusion; public disclosure of embarrassing private facts; false light publicity and appropriation of name or likeness. There was no attempt to link these separate torts by a coherent unifying principle. The Prosser approach was ultimately persuasive in the US. There is the argument also that privacy is in itself a property right. In this section, the emphasis will be on ‘personality’ interests rather than property rights in personal data.

Warren and Brandeis regarded privacy as a ‘right to be left alone’. But this description lacks content and boundaries. Theorists have attempted to remedy this deficit by defining privacy as the ability to limit the extent of access to self-suffer from similar difficulties. Gavison defines privacy as the right to limit ‘the extent to which we are known to others, the extent to which others have physical access to us, and the extent to which we are the subject of others’ attention’; privacy requires ‘secrecy, anonymity and solitude’. But not every access to the self-suffer results in a loss of privacy. For example, while the information itself may not be secret or anonymous as for instance, an e-commerce user’s purchasing preferences, the individual may nevertheless not want it to be disclosed to the entire world.

Recognising the right of an individual to control such information enables that individual to selectively restrict others from his or her physical and mental state, communication and information, and control how the person wishes to be presented, to whom and in which context. Rossler writes that:

---

10 Samuel Warren and Louis Brandeis, above n 6, 200.
11 The breaches of privacy as comprising four separate torts: invasion of seclusion; public disclosure of embarrassing private facts; false light publicity and appropriation of name or likeness are incorporated into the American Law Institute Restatement of Torts (2nd) under s 652B, s 652C, s 652D, s 652E, <http://cyber.law.harvard.edu/.../Privacy_R2d_Torts_Sections.htm>; See also Paul M Schwartz and Karl-Nikolaus Piefer, above n 9.
...the reason why the protection of privacy matters so much is that it is an intrinsic part of self-understanding as autonomous individuals within familiar limits to have control over their self-presentation, that is control of how they want to be presented or stage themselves to whom they want to do so and in which context control over how they want to see themselves and how they want to be seen.  

This control enables an autonomous individual to make choices, and to select those persons who will have access to their body, home, decisions, communication, and information and those who will not. In the context of e-commerce users, this approach would give users the right to determine who obtains information for what purposes. Clearly not all information of any kind would be subject to individual control. But what are the boundaries and what purposes would be served by those limits? If control were limited to personal information of an intimate nature, this would not extend to the vast array of information collected about e-commerce users and their preferences. Nor is the problem resolved by a broader and unbounded formulation of a right to control any information relating to the individual. Much information in the public domain would not be considered private and subject to individual control, for example, a person’s status or profession.

The search for a single definition which captures the essence of this right to privacy is elusive, and ultimately unproductive. As suggested by Solove, it is necessary to adopt a pragmatic approach to determine which privacy interests and concerns need to be addressed and how, within a particular context, rather than attempting a single unifying definition. Such an approach provides the opportunity to analyse and assess what is important and of value in a set of practices, as well as providing an aid to ‘solving problems, assessing costs and benefits and structuring social relationships’. Such an approach recognises that what is regarded as ‘private’ is not static with public and private sensibilities being moulded by an ever changing environment, and that privacy is a state that is variable over time and dependent upon context and that it may not be clear in

---

15 Beate Rossler, above n 3, 116.
16 Ibid.
17 Charles Fried, above n 5, 477.
19 Ibid.
advance how an individual’s view of privacy is to be weighed against other interests or what is to be weighed in that balance. The following paragraphs adopt Solove’s approach in analysing and assessing e-commerce practices, their costs and benefits and importance to e-commerce users. The emphasis will be on protection of ‘personality’ rather than the arguments whether an e-commerce user’s privacy rights could be regarded as some form of proprietary right in their own information.

Solove’s approach is in contrast to those of Warren and Brandeis, and later by Prosser, who saw privacy as a tortious remedy for an individual who suffered identifiable harm against an identified wrongdoer in relation to specified conduct, and whose enforcement depended upon the individual taking the necessary steps to do so. The limits of such an approach is, according to Solove, inadequate to deal with privacy breaches which are systemic and pervasive, and where knowledge is aggregated through a series of transactions as is the case with the vast sprawl of e-commerce.\(^{20}\) In relation to e-commerce users, the problem is that the aggregation of information paints pictures about individuals and their lives; the process may not be subject to external control and the user may be unaware of who or how or for what purposes the information will be used.\(^{21}\) Added to that harm may not be immediately identifiable and the individual disempowered from taking steps to protect individual privacy if the remedy is seen as torts based.\(^{22}\) This, Solove argues, requires thinking outside the traditional enforcement models and adopting new strategies to respond to the practices and environment under which e-commerce operates and shape its architecture.\(^{23}\) The design of the system should operate to limit invasions of privacy and to provide mechanisms to reduce risks of occurrence. In other words, unlike common law torts claims, the system should be designed to pre-empt privacy invasion. The chapter now turns to discuss the existence of a right to privacy.

---


\(^{21}\) Daniel J Solove, above n 18, 1154.

\(^{22}\) Above n 20.

\(^{23}\) Ibid.
3.3 The Right to Privacy

3.3.1 Rights

The term ‘rights’ generally denote entitlements and define what actions are proper and just.\(^\text{24}\) Traditionally rights have been understood as protecting an individual person against the incursions of the community based on the respect for the individual’s personhood, and autonomy and equality of respect. An individual who has a right must also have the ability to control and exercise authority over a certain aspects of his or her life, liberty, property and privacy that is linked to a right.

Hohfeld distinguished eight relations that are, claims, duties, liberties, no-claims, powers, liabilities, immunities and disabilities and identified four components of rights known as ‘Hohfeldian incidents’ that explains the relationship of rights and duties that arise when a claims right arises.\(^\text{25}\) A Hohfeldian ‘right’ refers to: 1) a claims-right by some person that some other person should do or refrain from doing something; or 2) a claim by some privilege, for example gives the privilege right holder the liberty to do or refrain from doing something. To say that someone has a certain claim right is to say that that person is owed an obligation by the other person to an act or omission. If an individual or group autonomously infringe upon the rights of others then they will be held responsible for the infringement.\(^\text{26}\) A claims right to privacy exists independently of anyone’s actions and an individual’s claim to privacy correlates to a duty in every other person not to abuse his or her privacy. A claim to ‘rights’ generally give rise to debates about ‘human rights’, ‘liberty’, ‘harm’, ‘benefit’, ‘fairness and justice’ and ‘equality’. A privilege right sets out what a bearer has no duty not to do; or 3) means a power that is the ability by acting or refraining from acting, to effect the legal relations of others; or 4) immunities.\(^\text{27}\) If all rights are nothing more than complex sets of obligations, powers, duties, and immunities, it would not automatically follow that we should dispense with talks of rights and frame our moral discourse in these more basic terms.

\(^\text{24}\) John Finnis, Natural Law and Natural Right (Clarendon Press, 1980) 206.
\(^\text{26}\) Wesley N Hohfeld, above n 25, 28-59; See also Wesley N Hohfeld, ‘Fundamental Legal Conceptions as Applied in Judicial Reasoning’ (1917) 26(8) Yale Law Journal 710.
\(^\text{27}\) Wesley N Hohfeld, above n 25.
The application of Hohfeld’s analysis of claims-rights in relation to privacy will mean that if individuals have a right to privacy then the State has a duty to protect that right. In short a right gives control,

…the to have a right is to have the ability to determine what others may and may not do, and so to exercise authority over a certain domain of affairs.\(^{28}\)

So this thesis argues that the State has a positive duty to protect privacy and that e-commerce users have a right to determine ‘what others may and may not do’ in relation to their personal information.

An autonomous individual exercising the right to be left alone is able to self-determine and make a choice whether to share sensitive information about them with others.\(^{29}\) The nature of the right is that it is always waivable. This is important when the issue of consent is considered in Chapter 4 and whether a privacy right should be waivable by consent. Will-based theorists are not always able to explain the function of rights where its holder has no power to waive the right. For example in circumstances when it is accepted that there is the unwaivable right such as not to be enslaved, or where persons are incapable of waiving rights such as infants and animals, or of those suffering from mental and physical incapacity although there is no doubt that they have rights.\(^{30}\) This is particularly important where individuals with a mental disability, the elderly, and children may lack capacity to consent to the collection, use or disclosure of personal information. In practice they are taken to have waived their rights by ticking a box agreeing to the terms and conditions of using a website. This is discussed in chapter 4. The current legislative frameworks assume that privacy rights can be waived by the individual user despite the problems of incapacity.

Basic human rights combine to set the minimum standards for preserving human dignity and equality. Individual autonomy and equality of respect is central to determining the


\(^{29}\) Samuel Warren and Louis Brandeis, above n 6.

nature and scope of individual rights and its protection.\textsuperscript{31} Liberal theorist, Joel Feinberg explains that:

\ldots the most basic autonomy-right is the right to decide how one is to live one’s life, in particular how to make the critical life-decision-what course of study to take, what skills and virtues to cultivate, what career to enter, whom or whether to marry, which church if any to join, whether to have children, and so on. \textsuperscript{32}

If the e-commerce user has a right to informational privacy, it may be qualified by the state exercising authority, through legislation, which trades off the individual’s rights as against broader public interest goals which may include commercial interests. But if informational privacy qualifies as a human right, it is arguably inviolable. The effect is that the State cannot deprive its citizens of their human rights for the benefit of the general community; a human right cannot be legislatively qualified. Despite pronouncements in international humanitarian laws such as the United Nation’s Universal Declaration of Human Rights (UDHR),\textsuperscript{33} and the European Convention on Human Rights (ECHR) that privacy is a human right, there is little consensus as to how it should be defined or what values are being protected.\textsuperscript{34}

\textbf{3.3.2 The Human Right of Privacy}

The two key issues here are whether an e-commerce’s right to information privacy qualifies as a human right. And if it does so qualify what is its effect? If it is inviolable, e-commerce users are entitled to privacy protection even if the maintenance of privacy imposes a cost on individuals, businesses, and the state. It is argued that if privacy is fundamental for the existence and dignity of a human being, then it should qualify as a

\textsuperscript{31} Wenar Leif, above n 28.
\textsuperscript{32} Joel Feinberg and Hyman Gross (eds), Philosophy of law (Wadsworth Publishing Company, 1986) 54.
\textsuperscript{34} Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, 4 November 1950, ETS 5 (entry into force 3 September 1953) <http://www.echr.coe.int/pathos/drefworld/docid/3ae6b3b04.html>. European Convention on Human Rights provides that: ‘Everyone has the right to respect for his private and family life, his home and correspondence’, art 8 (1), and that: ‘There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a domestic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others’ art 8 (2).
human right. The human right of privacy is seen as necessary for meaningful democratic participation and to ensure human dignity and autonomy and equality of respect. The right to privacy is no less a value than rights to self-determination, freedom of expression and thought that form the basic standards for human beings to survive and develop in dignity. So that, in an e-commerce context, an autonomous individual is able to decide and make a choice whether to share sensitive information about them with others.

If the privacy interest in personality is a human right and ‘inviolable’, these privacy interests in relation to intimate matters of private life are not balanced against public interest in information but are entitled to absolute protection. In short privacy in relation to private life in the civil arena is a human right not subject to takings by the State. This distinction is critical to an appreciation of the differences between Australian privacy protection and that of the EU. The EU adopts a human rights approach to information privacy, whereas the Australian legislative framework allows commercial interests to be traded off against the e-commerce user’s privacy rights. But not all scholars view human rights as ‘inviolable’ and trumping other societal interests.

This view of privacy as a human right does not permit the State to trade off the individual’s human rights against other interests. This contrasts with the utilitarian view of human rights. Rights such as freedom of speech, freedom from arbitrary arrest and privacy will only be protected by the utilitarian where that will maximise welfare overall. Utility does not take into consideration morality and justice and it is indifferent to theoretical problems that take into consideration the past but not the future. In contrast to individualism and communitarian concepts of individual rights, the utilitarian theory takes

37 For further details on Immanuel Kant (1724-1804) and his fundamental idea of ‘critical philosophy’ on human autonomy see Kant’s most notable written and published works that include: The Critique of Pure Reason (2nd ed., 1787); The Foundation of the Metaphysical of Morals (1785); the Critique of Practical Reason (1788).
the ultimate advancement of happiness, human welfare as the ultimate goal. Hume and Bentham believed that when a man desires something it is because he believes that it will bring him happiness. The utilitarian’s balancing of individual rights and the common good does not favour individual rights unless these interests advance the common good and society will succeed when its interests are balanced against those of the individual. The utilitarian takes account of everyone’s welfare or happiness rather than that of an individual and would licence any interference with liberty that was likely to improve overall welfare of society. Amitai Etzioni contends that privacy is ‘a societal license that exempts a category of acts (that is thoughts and emotions) from communal, public, and governmental scrutiny’ and that social interests should outweigh individual privacy interests. This argument supports the communitarian view that as soon as any part of a person’s conduct affects prejudicially the interests of others, society has jurisdiction over it. The European approach rejects this approach in its recognition that privacy is a human right which precludes its abridgement by other social interests. Directive 95/46/EC has as its objective ‘protecting the fundamental rights and freedoms of natural persons and in particular their right to privacy with respect to the processing of personal data’. The dominant approach to privacy as a fundamental human right is recognised in international human rights instruments discussed below at [3.4].

The ‘economic rights’ approach views information privacy not as a personality interest but as a property right in personal data. Viewed from this perspective, information privacy is an economic right that may be subject to be traded off against other economic interests in the interests of administrative efficiency. The economic argument assumes that property in information would be vested in persons to whom the data relates and that person could grant organisations consent or licence to copy, store, and use and/or disclose personal data

---

43 Ibid.
44 Daniel J Solove, above n 8, 760.
45 Nigel E Simmonds, Central Issues in Jurisprudence: Justice, Law and Rights (Sweet & Maxwell, 1986)
25.
48 See Directive 95/46/EC Art [1.1].
50 Ibid.
that has been collected about them as individuals. The emphasis in this thesis is on ‘personality’ interests and the use specific personal information about the individual.

If privacy constitutes a right inhering in the individual e-commerce user, the various theories all accept that it is waivable. The ability to waive one’s rights translates into allowing the individual to maintain a certain level of control over the inner spheres of personal information. But the difficulty is that even if it is acknowledged that the e-commerce user has a ‘right’ to privacy, once an individual ‘consents’ to the use of their personal information then they have waived their right to non-disclosure of that information. If a third party beneficiary processes their personal information from a primary data collector, e-commerce users lose their right to claim information privacy protection because whatever interest the user has in exercising his or her interest in their personal information, it has been waived as a result of the consent given for its collection, use and disclosure. The individual is then unable to ‘control’ how that information is to be used, and disclosed. Their personal information is under the control of third party beneficiaries. The problem for e-commerce users to consent and control their personal information, and the waiver of privacy rights in relation personal information of e-commerce users is discussed further in chapter 4.

3.4 Human Rights and Information Privacy

The e-commerce user’s right to protection against the unjustified invasion of privacy is reflected in the widespread adoption of some form of fair information practices. Fair information practices restrict collection, use, transfer and access to personal information. International human rights instruments provide a foundation for this protection.

---

51 Leaving aside the vexed question how one deals with individuals who do not have mental competence, see above.
52 The example given in the Stanford Encyclopedia is that ‘whatever interests a judge may have in exercising her legal to sentence a convict to life in prison the judge’s interests cannot possibly justify such a dramatic change in the convict’s normative situation’. See Stanford Encyclopedia of Philosophy: ‘Rights’ (Online) <http://www.plato.stanford.edu>.
53 The principle of fairness applies to individuals and requires that a person is required to do his part as defined by rules of an institution when two conditions are met. The first is that the institution or practices in question must be just (or fair); and secondly is that the act must be voluntarily accept the benefits of the arrangements or taken advantage of the opportunities to further one’s interests. The first principle sets the conditions necessary if these voluntary acts are to give rise to an obligation. H L A Hart, ‘Are There Any Natural Rights’, (1955) Philosophical Review 185 as cited in George C Christie and Patrick H Martin (eds), Jurisprudence: Test and Readings on the Philosophy of Law: American Casebook Series (West Publishing Co, 2 ed, 1995) 323.
3.4.1 International Human Rights Instruments

Since the early human rights declaration in Europe and in North America, there have been numerous treaties generally known as human rights instruments such as the Geneva Convention that was built on the Hague Convention 1899-1907 to safeguard the human rights of those involved in armed conflict.\(^{54}\) Humanitarian laws further developed with the Geneva Convention which came into being between 1864 and 1949.\(^{55}\) After the Second World War the protection of fundamental human rights developed further in response to the Holocaust which culminated in the signing of the Universal Declaration of Human Rights (UDHR) by the United Nations General Assembly in 1948.\(^{56}\) The articles (“arts”) of the UDHR recognise and endow individual rights to life, liberty, property in addition to spiritual, public and political rights, economic rights, social and cultural rights.\(^{57}\) The dominant approach to privacy protection in Europe is based on the concept that privacy is a fundamental human right; it is recognised in the key international humanitarian instruments such as the Universal Declaration of Human Rights (UDHR, 1948),\(^{58}\) the

\(^{54}\) Even more modern concepts of human rights to that of the sixteenth, seventeenth, and eighteenth century are generally classified under four groupings: civil and political rights, social and welfare rights, minority and group rights, and environmental rights. The various human rights instruments have expanded the basic rights of life, liberty, and property to now include civil and political rights, social and welfare rights, minority and group rights, and environmental rights. For example the Universal Declaration of Human Rights (UDHR) by the United Nations General Assembly in 1948; and International Covenant on Economic, Social and Cultural Rights (ICESCR) adopted and open for signature, ratification and accession by United Nations General Assembly resolution 2200A (XXI) of the 16 December 1966 entry into force 3 January 1976, in accordance with Article 27.

\(^{55}\) There were a series of conventions or amended conventions following the first Geneva Conventions the 1864 Convention. The 1864 Conventions was followed by the 1906 Convention, the 1929 Convention, and the current 1949 Convention.


\(^{57}\) Universal Declaration of Human Rights adopted by General Assembly resolution 217A (III) of 10 December 1948, Art 1. United Nations Universal Declaration of Human Rights (UDHR) states that, ‘All human beings are born free and equal in dignity and rights. They are endowed with reason and conscience and should act towards one another in as spirit of brotherhood’, (Art 1). The protection of fundamental human rights under national and international instruments will be discussed in the following chapters.

\(^{58}\) Art 12 of Universal Declaration of Human Rights (UDHR 1948) provides that: ‘No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.’
International Covenant on Civil and Political Rights (ICCPR, 1976),\(^{59}\) and the European Convention for the protection of Human Rights and Fundamental Freedoms.\(^{60}\)

The United Nations has adopted provisions for the protection of privacy under article (“art”) 12 of the Universal Declaration of Human Rights 1948; \(^{61}\) art 17 of the International Covenant on Civil and Political Rights (ICCPR); \(^{62}\) and art 16 of the Convention on the Rights of the Child were adopted by the United Nations. The relationship between the right to privacy and the right to protection against attacks on honour and reputation is clear from art 12 Universal Declaration of Human Rights and art 17 of the International Covenant on Civil and Political Rights (ICCPR). The ICCPR imposes a duty on all member nations to uphold the Covenants by ensuring adequate and effective protection against violation of privacy interests. The two treaties, that is the ICCPR and the International Covenant on Economic, Social and Cultural Rights (ICESCR)\(^{63}\) between them made the rights contained in the UDHR binding on all states that have signed this treaty creating human rights law.

Many international and regional treaties have been adopted into domestic laws art 12 of the Universal Declaration of Human Rights 1948; art 17 of the International Covenant on Civil and Political Rights; and art 16 of the Convention on the Rights of the Child provide that privacy is human right to be protected and given effect under the various international covenants. The European Convention for the Protection of Human Rights and

\(^{59}\) Art 17 of the International Covenant on Civil and Political Rights (ICCPR 1976).

\(^{60}\) European Convention for the protection of Human Rights and Fundamental Freedoms, Art 8 provides that: ‘1. Everyone has the right to respect for his private and family life, his home and his correspondence; and 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.’

\(^{61}\) Although the UDHR is a non-binding declaration, the third clause to its preamble indicates that the rights include in the UDHR are intended to be legally enforceable through some means. Clause three to UDHR reads, ‘Whereas it is essential, if man is not to be compelled to have recourse as a last resort, to rebellion against tyranny and oppression, that human rights should be protected by the rule of law’. See Preamble to the Universal Declaration of Human Rights (UDHR) 1948 adopted by the General Assembly resolution 217A (III) of 10 December 1948 <http://www.un.org/en/documents/udhr/index.shtml#al>.


Fundamental Freedoms also provides for basic human rights such as autonomy and respect, the right to life, liberty, security of persons, and the freedom from slavery and torture. These instruments provide the foundation for protection for a human right of privacy.

3.4.2 International Model Laws

At the international level organisations such as the Organisation for Economic Cooperation and Development (OECD), the European Union (EU), and Asia Pacific Economic Cooperation (APEC) have provided Model laws, guidelines and Directives for e-commerce. But the most important instruments which have influenced the international development of privacy regulation are the OECD Guidelines and the European Commission (EC) Directives. These are examined in detail in Chapter 5. The EC Directives give primacy to human rights over commercial interests. Indicative is the proposed Preamble to the Convention for the Protection of Individuals with Regards to the Processing of Personal Data which provides that:

...considering that it is necessary, given the diversification and intensification of processing and exchanges of personal data, to guarantee human dignity and the protection of human rights and fundamental freedoms of every person, in particular through the right to control one’s own data and the use made of such data.  

The Explanatory report to the Preamble to the Council of Europe’s Modernisation of Convention 108 comments that:

...human dignity implies that individuals cannot be treated as objects and be submitted to machines, and consequently that decisions based solely on the grounds of an automated processing of data cannot be made without individuals having the right to express their views.

---


66 Ibid, 8.
It reflects the view that the e-commerce user has a human right to privacy which is not subject to takings by the state in the form of legislation which qualifies that right. This contrasts with the Australian Privacy Act 1988 (Cth) which allows commercial interests to override individual privacy interests particularly in allowing direct marketing and secondary usage of e-commerce user’s personal data. This is explored further in chapter 6 at [6.2.2.2].

3.5 Conclusion

Privacy is an elusive concept and its definition difficult to capture. It contains many elements dignity, autonomy, personhood and the capacity to limit and control access to self. The emphasis in this chapter has been on these ‘personality’ interests and the e-commerce user’s right to be protected in relation to those interests. It has argued that the privacy of the ‘virtual’ person is important to protect personality interests. It has also been argued that the e-commerce user has a right to privacy that inheres in the individual and that this right qualifies as a human right based on inviolability of the individual. This is crucially important, because on one view, this inviolability means that the privacy rights of e-commerce users cannot be qualified by the state through legislation. Chapter 5 following will indicate that the EU position adopts this view of human rights in its provisions (see chapter 5 [5.5.3.1]). In contrast, chapter 6 observes that the Australian legislation, the Privacy Act 1988 (Cth) gives priority to commercial interests particularly in relation to direct marketing and secondary usage (see chapter 6 [6.2.2.2]).
Chapter 4: Consent and the Waiver of Privacy Rights

4.1 Introduction

The previous chapter examined the nature of privacy with particular emphasis on the protection of personality interests. The various iterations of privacy all accept that privacy inheres in the individual who may waive this right of privacy. The mechanism for waiving rights is through consent. This chapter examines the issue of consent. It questions the assumption in most legislation which affects e-commerce users, that consent is sufficient to waive privacy interests. It examines the role and meaning of consent. Viewed from the perspective of autonomy, it considers what autonomy means for these purposes and whether current practices (such as bundled consent) are consistent with individual autonomy. It then considers consent in the context of the contractual model. It observes that modern consumer protection law such as the Australian Consumer Law 2010 (Cth) provides protection to e-commerce consumers against unfair terms contained in standard form contracts. It then illustrates the potential application of the legislation in relation to e-commerce contracts. The Australian Consumer Law 2010 (Cth) assumes that outside standard form contracts (where consumers are not able to effectively bargain), consumers act as autonomous agents who are able to decide what is in their own best interests.

4.2 Consent

Consent is the expression of autonomy, the right for individuals to make decisions about how they will live their lives.¹ In this context, this chapter examines the e-commerce user’s consent to waive privacy rights. When a person exercises autonomy, to make decisions concerning themselves, what is required?² At its lowest, autonomy refers to liberty of action which is satisfied if the individual’s conduct is intentional and voluntary without coercion or duress. So that an e-commerce user who ticks the box agreeing to the conditions of usage without reading the conditions or privacy policy is exercising autonomy in this sense.

A secondary sense in which autonomy is used is that it requires freedom of choice. If the e-commerce user cannot access the services or website without agreeing to the terms and

² The principles set out are taken from Thomas A Mappes & David DeGazia, Biomedical Ethics (Mcgraw-Hill College, 4th ed, 1995) 25-29.
conditions, the e-commerce user’s choice will be constrained. Where an e-commerce user has a choice of supplier and is aware of the unfair nature of contract terms, the user can choose between suppliers. But this may assume a high level of sensitivity and commitment on the part of the e-commerce user in comparing privacy options of various suppliers. Moreover there is hardly a considered decision if the e-commerce user is required to immediately consent to complete the transaction.\(^3\) E-commerce users will often have no option but to consent to the collection and usage of their data if they wish to order or transact online. This is because in most cases if users do not comply with the service providers request to accept the terms of use, the user is not able to proceed further to access services or purchase online. In some instances, consumers may have to fill out an e-form with personal details before the Web site allows the user to access their services or search engine for information. Similarly if other providers have similar policies which do not allow the user to refuse the terms and conditions, the e-commerce user will lack autonomy in this secondary sense.\(^4\)

The third and most important meaning of autonomy, particularly where personal rights are involved, is that autonomy requires ‘effective deliberation’. It requires the individual to be a rational consumer making informed and considered decisions.\(^5\) The available evidence suggests that very few e-commerce users exercise autonomy in this sense; users seldom read privacy clauses on websites or change their behaviour as a consequence.\(^6\) It is argued

---

\(^3\) For example there are some businesses such as travel agencies that require Web site visitors searching for flight information, or competitive fares to provide personal information such as name, address, post code, contact details, e-mail address that are mandatory fields to fill in before they provide you with a quote. For an example see the travel agency, Flight Centre’s web site at <http://www.flightcentre.com.au>. If a visitor does not wish to provide such details but only to browse the website for information then the visitor is not able to access such information. The website provides an alternative option to phone in for more information but the consumer or user incurs a cost if they phone in for enquiries information. If a user does not wish to provide his or her personal information or incur a cost for the information searched for on the website the user has two other option that is to either to call the telephone number provided on the website and incur a cost to obtain that information or to go in person to the nearest agency office. It is highly likely that consumers will provide their personal information than take up the other two options.

\(^4\) This would not breach the NPPs as NPP2.1 (c)(iv) provides that if information is not sensitive and the use of the information is for secondary purposes of direct marketing if ‘the organisation draws to the individual’s attention or prominently displays a notice that he or she may express a wish not to receive any further direct marketing communications.”


that the e-commerce user’s ability to exercise autonomy as deliberative choice is constrained in a number of ways: first information may not be easily accessible. It may be difficult to find, in legal language which is not easily comprehended and may be lengthy and vague as to exactly what is being agreed. Users may be confused as to what rights they are actually surrendering. Secondly, e-commerce users’ choices may be constrained. They may be required to agree to terms and conditions up front to get access to the website and may find that alternatives are equally constrained. Viewed from the standpoint of individual privacy, legislation should ensure that constraints on the ability to make rational decisions are removed. There is the added problem relating to young persons and others who may lack legal capacity to consent. According to normal legal principles, consent cannot be effective if the person does not have sufficient knowledge or understanding to consent. The focus of this section will be on e-commerce users who have the capacity to consent.

This section now turns to look in greater detail at these constraints on the exercise of autonomy.

4.2.1 Knowledge

Consent is the mechanism by which the individual e-commerce user exercises control over the initial collection, use or disclosure of personal information. Before e-commerce users can make a considered decision whether to consent, they must have some understanding of the implications of what is being consented to, and sufficient detail in language suitable for e-commerce users to give genuine consent. First the e-commerce user must have sufficient knowledge and notice of the purpose for information collection, its use and disclosure of information collected; secondly, consent mechanisms should allow informed and rational decision making; thirdly, there should be the opportunity for individual choice allowing withdrawal of consent or the opting out of information collection.

The e-commerce user will not have the requisite knowledge of proposed use of personal information where data mining takes place. The problem with data mining is that the

---

that a privacy policy makes them more comfortable disclosing personal information while 73% of respondents indicated having viewed privacy statements in the past and 26% claim to always read them. Web site operators reported that the users hardly pay any attention to them. See also Florencia Marotta-Wurgler, ‘Does Disclosure Matter?’ (2010) New York University Law and Economics Research Paper No. 10-54 43.

organisation collecting personal information online from a website visitor does not identify what information is collected, the purpose for collection, how it will be used, or if it will be used and/or disclosed to third parties. Personal information collected through data mining is generally collected for secondary and future use.

Although broadly written ‘use statements’ could be added to customer agreements to allow data mining, whether or not these waivers are truly meaningful to consumers is doubtful. This is because data mining methods extract unknown patterns of information from a database.\(^8\) So individuals do not know and cannot know how their personal information will be used. There is less difficulty where the primary purpose of information use can be identified and where the use of that data is restricted to that particular purpose. For example, if the primary purpose of the collection of transactional information is to permit delivery of goods or a credit card payment, then using the information for other purposes without having identified this purpose before or at the time of the collection, is in violation of the purpose and use limitation principles.\(^9\) There is no objection where the primary purpose of the collection is notified and understood by the consumer and identified at the time of the collection.\(^10\)

The next section considers the use of standard privacy statements.

### 4.2.1.1 Standard-form Privacy Policy Statements

Privacy policy statements are used by ISPs, e-businesses and Internet websites. The purpose of privacy policy statements is to inform individuals of the type of information that is collected, the purpose for its collection, who is collecting such information, how that information will be used and if it will be shared with third parties. Privacy policies should also include information which alerts the e-commerce user to the right to obtain access, challenge and require correction of personal data.\(^11\) So privacy policy statements should provide contact details of the data collector to facilitate this.

---


\(^9\) Refer to chapter 6 [6.2.2.1], [6.2.2.1.1]. Information collected covertly through data mining will not comply with the requirements of the National Privacy Principles (NPP1.3 or NPP1.5).


Privacy policy statements may also serve a secondary purpose to give confidence to e-commerce users that their personal details will not be misused in purchasing, searching and browsing websites and engaging in e-commerce. Trust and risk are a major determinant of users disclosing their personal information to e-businesses. Various aspects of privacy statements on websites have been examined by researchers. These reports showed that ‘the willingness to provide information to online businesses increased as the level of privacy guaranteed by the Website’s privacy statement.’ According to these studies 76% of users find privacy policies very important and 55% stated that a privacy policy makes them more comfortable disclosing personal information. From those surveyed 73% of stated that they have read privacy statements in the past and hardly pay attention to them. A special report on the attitudes of Europeans towards data protection and electronic identity indicates that 74% of Europeans view disclosing personal data as being necessary and part of modern life. This suggests that users are only vaguely concerned about privacy.

Privacy decisions may have hidden transactions costs with e-commerce users wasting time looking for privacy policies that are linked to other organisation websites; policies may be lengthy and difficult to read. Statements regarding future possible usage may be vague and very general and hardly sufficient for the e-commerce user who does actually read them to be adequately informed and exercise a genuine choice. Generally these privacy statements are written in language not readily understood by an average reader. There is evidence that indicate that consumers generally do not read their e-standard forms and a
few that do not read beyond price and description of the goods or services. Researchers looked at online privacy policies and how long it takes to read them found that while one policy had just 144 words another had 7,669 words in around 15 pages. The average length of privacy policies used by 75 most popular U.S. websites is 2,500 words and takes about an average of 10 minutes to read. It was estimated in the same research that it costs US citizens to read every privacy policy they visit once a year if the time was charged a cost of $652 billion a year. Evidence shows that e-businesses such as Amazon, search engines such as Yahoo and Google, and social networking websites such as ‘Facebook’ have come under fire from watchdog groups for displaying inconsistent and hard-to-understand privacy policy statements.

A more significant problem arising from inconsistent and hard-to-understand policy is illustrated for example when a person purchasing a mobile phone service will need to have Internet access to find out whether the printed policy included with the product purchase has been changed. Privacy policies may state that the policies are changeable without notice let alone prior notice. It is also common for providers to inform its customers in the company’s ‘Privacy Statement’ that their privacy policy may change as their business requirements or the law changes. The statement may inform an e-commerce user that any changes to this Privacy Statement will be updated on the company website. There are illustrations in the public domain where providers changed policies without notice and were subsequently forced to change policies allowing access to personal information even if the user had consented to terms and conditions of use. For example in a case involving a 13 year old minor who had provided personal information to ‘Facebook’ when registering with the social networking website, Facebook changed its privacy policy without notice and disclosed the minor’s personal information without notice or consent. 'Facebook' was sued for violating California consumer privacy laws when personal information relating to the 13 year old minor was accessed and used for secondary purposes.

---

20 See Out-Law.com, above n 17.
21 Roger Clarke, above n 6.
reverted to its old policy. Very often privacy policies from e-businesses are undated and may not highlight changes made since the previous version. So that even fully informed, rational e-commerce user would need to visit the website periodically to ensure up to date information on the privacy policy.

Another problem is that although organisations may provide details of the organisation’s privacy policy on its website this does not guarantee compliance with privacy policy statements. For example Google was severely criticised for failing to post a homepage link to its privacy policy. The reason given by Google for non-compliance with the law was that it did not want to clutter its homepage. There are significant barriers to the effective exercise of autonomy when e-commerce users have difficulty in locating the provider’s privacy policy. There may be no direct link to the policy or the link may not work. It is not simply a problem with small e-commerce vendors.

In Australia, the Privacy Act 1988 (Cth) makes no specific requirements about the posting of privacy policies and access to those policies. The National Privacy Principles (NPPs) promulgated under that Act. NPP1.3 requires an organisation that collects personal information about an individual from an individual to ensure that the organisation at or before the time (or, if not practicable then as soon as practical after) take reasonable steps to make the individual aware of the identity of the organisation, its contact details, how the individual can gain access to the information collected, the purpose for which the information is collected, the type of organisations to which the organisation usually discloses information of that kind, if the collection of such personal information is required by law, and the main consequences (if any) for the individual if all or part of the information is not provided. This will be discussed in detail in chapter 6 at [2.2]. The lack of specific requirement under the Australian provisions for posting of privacy policies is in contrast to California’s Online Privacy Protection Act 2003 (‘OPPA’).


25 Privacy Act NPP 1 and NPP 2 reflect the OECD principles on collection limitation, and use limitation. NPP1.5 provides that if the information about the individual is collected from someone else then the organisation collecting such information must comply with the requirements under NPP1.3 except if making the individual aware of the matters would pose a serious threat to the life or health of any individual; Refer to the extract of the NPPs in Appendix 3.

26 California Online Privacy Protection Act 2003 (‘OPPA 2003’) (U.S.) came into effect on 1 July 2004.
Privacy Protection Act 2003 (‘OPPA’) provides that all owners of commercial Web sites or online services involved in personal information collection from Californian residents must: conspicuously post their privacy policies on their websites and comply with those posted policies. It also provides specific guidelines as to what is required. Commercial Web sites must disclose in the privacy policies the types of personally identifiable information (that information which allows a visitor to be individually identified, such as name, e-mail, physical address, etc.) collected, and must identify, generally, any third parties with whom that information might be shared, and under what circumstances. Owners of commercial Web sites are also required to provide a description of the process (if one exists), by which a visitor can request changes to any of that information; describe the process by which the operator of a Web site notifies users of changes to that privacy policy; identify the effective date of the privacy policy. Violators will be notified and given 30 days to comply. Those who still fail to comply with the provisions of OPPA would be subject to civil suit for unfair business practices.

The exercise of autonomy by an e-commerce user is constrained when privacy policies are difficult to access, in language that is not appropriate for the ordinary website user and where the user frequently has little option but to consent to the conditions imposed for use of the website.

4.2.1.2 Choice and Opt-in and Opt-out

This section examines the importance of choice in the exercise of individual autonomy. Two issues are considered: first where the e-consumer effectively does have a choice whether to consent; and secondly, the use of opt-in and opt-out mechanisms for securing consent.

Almost all fair information practices such as for example the OECD’s Collection Limitation principle, Directive 95/46/EC, Articles 7, 14, and Privacy Act principles NPP1 and NPP2 have as their foundation consumer choice or consent as an essential element. Under these fair information practices, the individual consumer chooses whether to engage in a relationship or receive communications. So choice means giving e-commerce consumers options in relation to their personal information.

27 Refer to chapter 5 [5.2.1], [5.3]; see also chapter 6 [6.2.2].
E-commerce websites may offer choice based on an opt-in or opt-out model. The opt-in regimes require positive action by the consumer to allow the organisation to collect and use their personal information.\(^\text{28}\) The opt-out regimes require positive action to prevent the collection and/or use of such information. If consumers do not actively select opt out, then they are taken to agree by default. Consumers may unwittingly agree to the default rule by not noticing the opt-out box particularly where this is not drawn to their attention prior to completion of the transaction. On one view this could be considered consent by trickery. The box may be ticked as the default state to indicate agreement with the consumer required to ‘untick’ the box if they do not agree. The choice may not be prominent and can be easily overlooked. On one view it is not a true choice. Choice can also involve more than a binary yes/no option. For example the options commonly available on most websites include, (1) do not allow any data mining, (2) allow data mining only for internal use only, or (3) allow data mining for both internal and external use.\(^\text{29}\)

In the above example, the consumer only has three choices and no other options are available to them. Internal in the third option refers to the use of data mining technologies such as cookies that perhaps record personal details and number of visits for the organisations internal use. External use refers to data mining with the purpose of transmission to a third party that has no link to the user.\(^\text{30}\) While views differ on the efficacy of the opt-in versus opt-out regime,\(^\text{31}\) a useful compromise will be for sensitive information to be subject to an opt-in regime, and for less sensitive information to be subject to an opt-out regime. This of course raises the question whether e-commerce users should be so restricted in the choices they may make.

Arguably data mining eliminates the possibility of an e-commerce user making a choice. If data mining is to fall into line with fair information practices then consumers must be

---

\(^{28}\) For an example of positive opt-in regime on a travel agency website see the Website for Flight Centre, Australia at <http://www.flightcentre.com.au>.


\(^{30}\) Ann Cavoukian, above n 8.

\(^{31}\) People are also less likely to opt out if consent is asked for before choices are offered. Ann Cavoukian states that studies show that there is less concern expresses by individuals when their personal information is used by a company that has collected primary data and if that primary data is used for secondary purpose within its own organisation but that there is far greater resistance to having data disclosed externally for use by unknown parties. Ann Cavoukian, above n 8, 16; See also Roger Clarke, ‘Privacy and Dataveillance, and Organizational Strategy’ (Xamax Consultancy Pty Ltd, 1997) <http://www.rogerclarke.com/DV/PStrat.html>. A framework to guide businesses and governments towards adopting a strategic approach to privacy is provided in this paper.
aware that a business that they are transacting with could be carrying out data mining activities. This knowledge for some consumers will make no difference while for others it is a matter of concern. For example if e-commerce users know that data mining occurs on a web site then they may decide what matters, and based on that, what choices they want to make about assuming control over the uses of their personal information. Concerned consumers may choose to take responsibility by informing businesses of their requirements and expectations regarding privacy as to whether they expect:

1. to be informed of any additional purposes that their personal information may be used for beyond the primary purpose of the transaction, or the option to deny secondary or additional uses of your personal information (this option is usually provided in the form of opting-out of permitting the use of a consumer’s personal information for additional secondary uses or an opportunity to ‘opt-in’ to secondary uses);

2. a process to be in place which gives them the right to access any information a business has about you, at any point in time; or

3. a process that permits them to challenge, and if successful, correct or amend any information held by a business about you, at any point in time; or

4. an option to have their personal information anonymized for data mining purposes and/or, an option to conduct your transactions anonymously.\(^{32}\)

Consumers can then decide what course of action if any, to take. It is arguable that individual autonomy and choice is more effectively provided if e-commerce consumers are allowed to tailor the nature of the information they reveal and the uses to which it may be put. Such an approach puts a premium on individual choice and privacy but probably at some cost of efficiency for the e-commerce provider as well as a heavier onus on the user to so choose.

### 4.2.1.3 Bundled and Blanket Consent

The capacity of the e-commerce user to exercise autonomy is further compromised by the use of bundled or blanket consent used by data collectors and e-business operators. Bundled consent refers to the consent to a wide range of uses and disclosures without giving an individual the opportunity to make a choice about which use or disclosure they

\(^{32}\) Ann Cavoukian, above n 8, 15.
agree to and which they do not. It is also common for data collectors to require bundled ‘consent’ for e-commerce users so that they may use and disclose personal information within their organisation and also with branches of their organisation overseas and with other third parties. Bundled consent frequently includes terms and conditions allowing changes to privacy policies without notice. The use of bundled consent cannot be meaningful. As indicated earlier, the person who consents to such terms and conditions does not necessarily know what he or she is consenting to. The person usually does not have a choice to opt out or to opt in.

In summary, it is recommended that owners of commercial Internet web sites or online service providers conspicuously display their privacy policies on their websites and include in it categories of personal information that will be collected from customers, the type of information that will be or may be shared with third parties, a description of the process through which customers may access and change incorrect personal information and when website owners or service providers allow such changes, the process through which customers will be notified of any material changes to their privacy policy, and identify the effective date of their privacy policy. This measure will not only provide notice but allows customers and users to be aware of how their personal information will be collected and used and give users options regarding how a company collects their personal information and if it will be used for secondary purposes. Customers and users may then take affirmative steps to opt-in or opt out from allowing the collection and/or use their personal information. Any choice command should also give customers and users simple and easy steps for customers to follow so that they can exercise their choice. One way would be to link the customer to online privacy policies to the choice/consent form on websites. Privacy policy statements must also accurately describe the steps consumers may take to access their personal information, the cost if any, the time expected to take the consumer to receive access after making the request, the means to contest inaccurate or incomplete data about them and to delete data or discontinue the use of personal information. These recommendations will best reflect a consumer’s autonomous choice whether to waive their privacy rights.

33 Some websites specifically inform customers what a privacy statement is; why it has one; what obligations it has under the Privacy Act; if it collects general information; if it collects personal information; if the information collected is only for internal use or if it shares personal information with other companies; if they ensure confidentiality of information by using encryption; how the customer can access, update and
This section has examined express consent but it should be noted that under the Privacy Act 1988 (Cth) and NPPs, consent can be express, implied or inferred from previous transactions and conduct. The circumstances where information may be disclosed without consent and implied or inferred consent are discussed in chapter 6.\(^{34}\) Currently neither the Privacy Act 1988 (Cth) nor the NPPs have provisions that prohibit bundled consent.\(^{35}\) So technically, since consent has been obtained there is no breach of the e-commerce user’s privacy. But, as has been argued, in the absence of informed choice, consent is hardly meaningful and, in the circumstances, ought not to be sufficient to waive privacy interests. This broader view accords with the current trends in consumer protection in which legislation recognises the unequal bargaining power of consumers in entering into contracts and where Courts may intervene even where the consumer has agreed to terms and conditions imposed by a provider. The obligations of data collectors to obtain the consent of data subjects prior to personal information collection under the Privacy Act 1988 (Cth) and associated National Privacy Principles (NPPs) is discussed in chapter 6 [6.2.2.1.1].

The previous discussion assumed that it is sufficient for e-commerce users to be bound that they have consented. But as will be seen in the discussion following modern consumer law recognises that in some situations, particularly, where there is inequality of bargaining power, agreements can be set aside despite consent.

**4.2.2 Consent and the Contractual Model**

**4.2.2.1 The Role of Consent in Contractual Settings**

The traditional contractual model is based on bargains reached by autonomous agents. Its assumption of equal bargaining at arm’s length belies the experience of modern day consumers who operate in a take or leave it environment. Consumer protection law recognises that consumers are frequently disadvantaged in a relationship where the terms

---

\(^{34}\) Refer to the discussion in chapter 6 [6.2.2.1.1], [6.2.2.2.2]. Privacy Act 1988 (Cth) NPP1.2 provides that personal information should only be collected by lawful and unfair means and not in an unreasonably intrusive way but does not provide that consent must be obtained prior to data collection. Under NPP2 a data collector must not use or disclose personal information without consent but exceptions exist.

\(^{35}\) The NPPs under the Privacy Act 1988 (Cth) only provides for how their personal information is to be handled and requires consent to the collection of personal information, its use and disclosure to others and right to access and to correct inaccurate information about oneself.
and conditions are set by powerful commercial interests, where there is inequality of bargaining power and where the consumer lacks information upon which to make an informed choice. The problem is not just one of information asymmetry where the consumer does not have adequate information to make rational choices. The issue is important here as privacy clauses and consent to collection, use and disclosure of information can form part of the terms of the e-commerce contract. Under classical contract law courts do not invalidate a contract purely on the grounds that the contract or its terms are unfair. At common law, in the absence of duress, undue influence or unconscionable conduct, courts would not set aside a bargain. It is, however, apparent in modern day legislation regulating standard form consumer contracts, that a strict contractual model may no longer be applied.

The next section reviews privacy waivers by e-commerce users in standard form contracts. It argues that Australian legislation now recognises that consumers do not have equal bargaining power with big business and are often not given the choice whether to accept unfavourable contractual terms. It lays the foundation for the argument that consent should not necessarily be regarded as sufficient to surrender privacy interests.

4.2.2.2 Standard Form Contracts

In e-commerce, consumer transactions are usually governed by standard form contracts. Standard form contracts may benefit parties to a contract by reducing transaction costs and time associated with negotiating individual contracts. When e-businesses offer specific terms to e-commerce users for the purchase of goods and services which the user agrees to, they usually form part of the terms of the e-contract binding both the e-business and the consumer. The most common presentation of terms of contract on a web-page to continue


At common law, the unconscionability doctrine was very limited. Unconscionable conduct occurs if one party to a transaction is at a special disadvantage in dealing with the other party and the other party takes advantage of this opportunity. See Bromley v Ryan (1956) 99 CLR 362. See also Commercial Bank of Australia Ltd v Amadio (1983) 151 CLR 447.

So, for example, in high pressure selling situations, it is not uncommon to find cooling off periods allowing the consumer to withdraw from a contract within a defined period or contract terms which cannot be excluded.


purchasing goods and services is accepted by the consumer clicking the ‘I accept’ button. These online contracts are often referred to as ‘click-wrap’ agreements’. \(^{41}\) ‘Clickwraps’ contracts enable mass marketing of goods and services. Vendors offer one-size-fits-all terms and conditions to consumers and there is no way to negotiate terms individually. \(^{42}\) Some examples of standard form contracts that relate to e-commerce include: banking and financial services, loans, and credit card contracts; software licences; online sales (eBay, iTunes etc.). Consumers may agree to terms and conditions and privacy policies by visiting commercial websites, media organisations, and social networking websites. It can be argued that even if no product is purchased, a contract is in existence. There is offer and acceptance supported by consideration – the user obtaining the benefits of use and access in return for agreeing to the terms and conditions. In this context, e-commerce users enter into bargains based on their agreement (consent). E-commerce users in purchasing goods and services online may be contractually bound by terms and conditions relating to privacy.

### 4.2.2.3 Australian Consumer Law

In Australia standard form contracts \(^{43}\) are subject to consumer protection provisions under the Competition and Consumer Act 2010 (Cth). \(^{44}\) The recent amendments affect all consumer e-contracts by providing for non-excludable conditions and warranties whereby any terms of contract that has the effect of excluding, restricting or modifying rights or liabilities under these implied terms will be void. The unfair contract provisions \(^{45}\) apply to

---


\(^{42}\) Above n 39, 437–40.

\(^{43}\) Competition and Consumer Act 2010 (Cth) sch 1 s 7 provides a list of factors that can be taken into account in determining if a contract is a standard form contract. These are: ‘(1) If a party to a proceeding alleges that a contract is a standard form contract, it is presumed to be a standard form contract unless another party to the proceeding proves otherwise; (2) In determining whether a contract is a standard form contract, a court may take into account such matters as it thinks relevant, but must take into account the following: (a) whether one of the parties has all or most of the bargaining power relating to the transaction; (b) whether the contract was prepared by one party before any discussion relating to the transaction occurred between the parties; (c) whether another party was, in effect, required either to accept or reject the terms of the contract (other than the terms referred to in section 5(1)) in the form in which they were presented; (d) whether another party was given an effective opportunity to negotiate the terms of the contract that were not the terms referred to in section 5(1); (e) whether the terms of the contract (other than the terms referred to in section 5(1)) take into account the specific characteristics of another party or the particular transaction; (f) any other matter prescribed by the regulations.’

\(^{44}\) The Trade Practices Act 1974 (Cth) has since been reformed in two stages. The Trade Practices Amendment (Australian Consumer Law) Act (No 1) 2010 (Cth) came into effect on 1 July 2010. The second stage of the reforms to the Trade Practices Act 1974 (Cth) contained in the Trade Practices Amendment (Australian Consumer Law) Act (No 2) 2010 (Cth) which came into effect on 1 January 2011. The Trade Practices Act has been renamed the Competition and Consumer Act 2010 (Cth).

\(^{45}\) Competition and Consumer Act 2010 (Cth) sch 2 Australian Consumer Law s 23 provides for unfair contract terms while s 25 provides examples of unfair terms and s 8 excludes the unfair contract terms related
any standard form consumer contract which is entered into, renewed or varied from 1 July 2010. At the federal level, prior to the introduction of the new Competition and Consumer Act 2010 (Cth) Sch 2 Australian Consumer Law, there were no such provisions directly dealing with unfair standard form consumer contracts. In so far as agreement to privacy clauses and the like are contractual in nature, the new law may provide an avenue for redress if these clauses result in the contract being unfair. Under the provisions, a court may set aside a standard form contract on the ground that is unfair. The Courts may consider the terms of the contract as a whole; the extent to which the term is transparent; if the standard form contractual terms of the contract cause detriment, financial or otherwise to the consumer if it were to be applied or relied on; and if the terms are reasonably necessary in order to protect the legitimate interest of the party who would be advantaged by the term.

4.2.2.4 Unfair Contracts

The unfair contract terms provisions apply to standard-form consumer contracts. The Competition and Consumer Act 2010 (Cth) Sch 2 Australian Consumer Law does not specifically define what constitutes a 'standard form contract' but the guidelines on Unfair Terms suggests that unfair terms relate to ‘take-it-or-leave-it’ contracts, prepared by one party, which cannot be negotiated. The Competition and Consumer Act 2010 (Cth) Sch 2 Australian Consumer Law defines a term as being an unfair term if it would cause a significant imbalance in the parties' rights and obligations under the contract; if it is not reasonably necessary to protect the legitimate interests of the party who would be advantaged by the term; and if it would cause detriment to a party if it were to be applied and relied on. In determining if the terms are unfair, it is the substance of the terms and the

to for example insurance contracts under the Insurance Contracts Act 1984, and companies and managed investment schemes. Section 20 of the Act prohibits unconscionable conduct and contracts but it is unlikely that e-commerce contracts will come within its purview. At common law unconscionable conduct occurs if one party to a transaction is at a special disadvantage in dealing with the other party and the other party takes advantage of this opportunity. See Bromley v Ryan (1956) 99 CLR 362 per Kitto J.

Besides the Competition and Consumer Act 2010 (Cth), the Fair Trading Acts in the States and Territories and Misrepresentation statutes may provide some remedies. See Fair Trading Act 1987 (NSW) s 57 on unconscionable conduct in business transaction; Misrepresentation Act 1972 (SA) s 7; Civil Law (Wrongs) Act 2002 (ACT) s 175.

Competition and Consumer Act 2010 (Cth) sch 2 Australian Consumer Law s 24 (1); See also Jeannie Paterson, above n 36.

Competition and Consumer Act 2010 (Cth) sch 2 Australian Consumer Law s 24 (1)(c).

Ibid, s 24 (1)(b).

Ibid, s 3 defines the meaning of ‘unfair’, s 4 provides examples of unfair terms, and s 7 provides for factors to be taken into account in determining if a contract is a standard form contract.
behaviour of the contracting parties that is important. Fair dealings should require a vendor not to deliberately or unconscionably take advantage of the consumer’s necessity, indigence, a lack of experience, unfamiliarity with the subject matter of the contract, weak bargaining position, and any other relevant factor.

In determining whether the contract is unfair, the following are to be taken into consideration: (1) there was an imbalance in bargaining power; (2) the contract was prepared by one party before any discussion concerning the transactions occurred; (3) a party was required to accept/reject the contract terms in the form they were presented; (4) a party was given an effective opportunity to negotiate the terms of the contract; and (5) the terms of the contract take into account the specific characteristics of a party or transaction.

If it is determined that the standard form contract is unfair then the unfair contract term is void and a person has access to any remedies which may apply under the common law. For the purposes of the Competition and Consumer Act 2010 (Cth) Schedule 2 Australian Consumer Law, certain other remedies are made available, namely injunctions; compensation orders; and orders for the provision of redress to non-parties.

The following section examines if the threshold test for unfair contract terms can be applied to ‘clickwrap’ contracts used in e-commerce. It has been noted above that these contracts may include bundled or blanket consent, privacy policies that are difficult to locate or which may be changed at any time without notice and where the consumer may have little choice but to accept.

---

51 Competition and Consumer Act 2010 (Cth) sch 2 Australian Consumer Law s 25 provides examples of unfair contractual terms. For further discussion on the threshold test for unfairness terms refer to Jeannie Paterson, above n 36.
52 Jeannie Paterson, above n 36.
53 See Kowalczyk v Accom Finance Pty Ltd (2008) 252 ALR 55 for issues that raise substantive unconscionability; See also Jeannie Paterson, ibid.
54 Competition and Consumer Act 2010 (Cth) sch 2 Australian Consumer Law s 27(2).
55 Ibid, pts 2, 3.
4.2.2.5 Unfair Terms and Standard Form ‘Clickwrap’ Contracts

In relation to the five factors that are relevant to a finding of unfairness, it is clear that in the usual e-commerce transactions, there is an imbalance in bargaining power; the contract was prepared without any negotiation between the parties; the e-commerce user was presented with an accept/reject choice only and there is no opportunity for negotiation or tailoring of the contract to the special requirements of the e-commerce user. So in relation to the standard form ‘clickwrap’ e-contract reflects a significant imbalance in bargaining power on the part of the consumer.

Online contracts such as ‘clink-wrap’ agreements lack the bargaining process that is present between contracting parties when there is a formal ‘meeting of the minds’. In online contracting the consumer is presented with long and often complex list of terms and conditions that they must scroll through before presented with an option to click ‘I agree’ or ‘I disagree’. If the consumer clicks on the ‘I agree’ button the contract is formed but when the consumer chooses the ‘I disagree’ button then a reminder to click pops up on the computer screen and this is followed by the website removing any further attempts to disagree. Users have no option but to tick the ‘I agree’ box that have privacy clauses that are included as part of the terms and conditions of an e-contract. In e-commerce, network systems often do not allow user access or an option to negotiate or modify mandatory fields such as where the identity of the user, e-mail address, telephone number where a user does not have an option to opt out of giving such personal information. Such ‘take it or leave it e-contracts are characteristic of contracts that lack bargaining power for consumers.

It may be argued that these characteristics of e-commerce contracts give rise to unfair terms which may be declared void under the Australian Consumer Law. The importance of

---

56 ‘Clickwraps’ contracts might sometimes give rise to misleading or deceptive conduct in relation to privacy policy statements or a website or if it is unclear when the customer connects from one website to another. Websites use internal and external links, frames, tags, location and prominence of disclaimers and content and these must not be misleading or deceptive. Competition and Consumer Act 2010 (Cth) sch 2 Australian Consumer Law s 18, now provides for misleading and deceptive conduct. The Australian Competition and Consumer Commission (ACCC) (the regulator for the Trade Practices Act 1974 (Cth), now the Competition and Consumer Act 2010 (Cth) has investigated Google Australia and Trading Post for allegedly disguising paid advertising as legitimate search result.

57 For further details see the website of the Consumer Law Centre, Victoria, Standing Committee of Officials of Consumer Affairs Working Party on Unfair Contracts Terms: Unfair Contract Terms-A Discussion Paper (January 2004) 17. The widespread usage of unfair contracts terms was also discussed in the submission of the Australian Consumer’s Association to the Dawson Inquiry into the Competition Provisions of the Trade Practices Act 1974 by the Australian Consumers’ Association.
this is twofold: first, in standard form modern consumer contracts, consent (agreement) is not the determinative factor; secondly, the legislation provides a potential remedy for consumers whose privacy has been infringed.

4.3 Conclusion

This chapter has examined express consent as providing the basis for an e-commerce user’s agreement to the collection, use, access and transfer of personal information. The discussion makes clear that consent should be regarded as being instrumental to individual autonomy. The discussion highlights the three senses in which autonomy is being used. In relation to e-commerce users, the legislative framework can be satisfied if the user has liberty of action, that is, if the user agrees without duress or coercion. Autonomy is only truly observed if the e-consumer has both choice and the opportunity to make rational and informed decisions. Although it is not possible to ensure that a consumer will act rationally with informed consideration before deciding to waive their privacy rights, the legislature can, at least, legislate to remove constraints preventing informed and rational decision making. The point is also made that an appropriate regulatory response will be to remove constraints which impede considered decisions about privacy by e-commerce users. Objectionable from this point of view is the difficulty of finding and understanding information relating to privacy policies, blanket or bundled consents, the lack of choice whether to accept conditions and the preference give to commercial interests in the current legislative regime.

As discussed above at [4.2.1.1], standard form privacy policy statements and fair information practices require that when there are any changes to an organisation’s privacy policy the website user should be alerted to this change with information which includes the date of issue and a list of changes made by the organisation to the prior version. Australian legislation should explicitly enact a provision similar to that in California noted above. It is also recommended that the Australian federal government similarly provide in the Privacy Act 1988 (Cth) that all owners of commercial Web sites or online services involved in personal information collection display or conspicuously post their privacy policies on their websites and comply with those posted policies. The Australian Law

Reform Commission in its Report 108 (2008) recommends that privacy policy statements disclose the consequences, if any, of an individual's refusal to provide information; and to include a clear statement of what accountability mechanism the organisation uses, including how to contact the organisation.

Viewed from a contractual perspective, a strict contractual model is out of step with modern legislation protecting consumers. The terms and conditions under which e-commerce users buy goods and services, especially the non-negotiability, the terms of contracts which favour the vendor, the location of the e-contract in a jurisdiction that suits the vendor, the lack of consumer protection that the customer may normally enjoy when purchasing goods and services in their home jurisdiction and security of personal information related to the e-commerce user’s personal data such as identity, and credit card details. There is obvious disparity in the power to negotiate between the vendor and the customer in standard form ‘clickwrap’ contracts. Users have limited or no negotiating power over the terms of the contract. There is also little opportunity for the consumer to read, understand or take advice on the terms of the contract. Such standard form contracts offer little potential for genuine consent on the part of the consumer. In this context it would appear that the Australian legislation dealing with unfair standard form contracts, takes the position that a consumer is unfairly disadvantaged when there is little choice on whether to accept unfavourable terms in dealing with an e-commerce provider. Thus, an e-commerce user should only be regarded as accepting the terms of privacy policies and collection and usage policies if the information is easily found, set out unambiguously with the consumer being given every opportunity to refuse to agree to collection of personal information except in so far it is essential to the transaction. It will

61 The Australian Law Reform Commission and the New South Wales Law Reform Commission have examined the obligation of public sector agencies and private sector organisations to ensure that data subjects are aware of certain matters when their personal information is being or has been collected. It was noted that notices may not reflect usage for secondary purposes commented upon. If there also is no mandatory requirement for a privacy policy statement to include information related to the purpose of data collection, how it will be used or a guarantee to process personal information fairly. The New South Wales Law Reform Commission concluded that notification is one way of achieving awareness. This research agrees with the above mentioned recommendations made by the Australian Law Reform Commission, and the New South Wales Law Reform Commission. For further details refer to Australian Law Reform Commission, ibid [23.1]; see also New South Wales Law Reform Commission, Privacy Principles, (Report 123) (2009); Privacy Alliance, Guidelines on Privacy Policies (2010) <http://www.privacyalliance.org/resources/ppguidelines.shtml>.
be later shown in chapter 6 at [2.2.2.1], that a system similar to that prevailing in the European Union that requires registration prior to collection and usage of data should be adopted.  

Consumers and data collectors could be required to engage in a form of ‘electronic negotiation’ regarding the scope of information that can be used and disclosed. The World Wide Web Consortium (‘W3C’) has developed the Platform for Privacy Preferences Project (‘P3P’), which will allow implementation of such technology. So consumers can be provided separate choices as to whether they wish to be on a company's general internal mailing list or a marketing list sold to third parties. In order to be effective, any choice regime should provide a simple and easily-accessible way for consumers to exercise this choice. This gives preference to individual privacy interests over commercial interests.

The next chapter examines the Organisation for Economic Co-operation and Development (OECD) and European Union provisions in the light of the discussion in chapter 3 whether the right to information privacy is protected as a human right and how far commercial interests are permitted to override personal privacy interests.

---

63 Directive 95/46/EC art 18, requires that the controller or his representative, if any, must notify the supervisory authority before carrying out any wholly or partly automatic processing operation or set such operation intended to serve a single purpose or several related purposes.

64 For general information on P3P refer to the W3C’s Web site <http://www.w3.org/P3P>.
Chapter 5: Informational Privacy-the OECD and EU Norms

5.1 Introduction

The previous chapters have examined whether e-commerce users have a right to privacy which protects personal information against the unauthorised access by others and the problems with allowing use and disclosure of personal information based on consent. This chapter examines the two key international approaches to protection of information privacy: the Organisation for Economic Co-operation and Development (hereafter referred to as ‘OECD’) Guidelines and the European Union (hereafter referred to as ‘EU’)’s European Commission (hereafter referred to as ‘EC’) Directives. The current information privacy protection laws in many jurisdictions are broadly based on the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (hereafter referred to as ‘OECD Guidelines’), the Council of Europe’s 1981 Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No.108) (hereafter referred to as ‘Convention 108’), and the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regards to the Processing of Personal Data and on the Free Movement of Such Data (Eur. O.J. 95/L281) (hereafter referred to as ‘Directive 95/46/EC’).

A threshold issue recognised in both the OECD Guidelines and the EC’s Directive has been the need for flexibility to accommodate the needs of individual countries while at the same time ensuring a degree of uniformity as between these jurisdictions. The need for some level of uniformity was apparent given that both individual privacy as well as efficiency would be compromised if there were differing legislative requirements in OECD member states. In other words, without some level of uniformity the free flow of information would be inhibited with the possibility of causing serious disruption to important sectors of the economy, such as banking and insurance. These considerations

---

1 Refer to chapter 3 [3.3], chapter 4 [4.2].
2 The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No.108) (‘Convention 108’), drawn up within the Council of Europe by a committee of governmental experts under the authority of the European Committee on Legal Co-operation (CDCE), was opened for signature by the member States of the Council of Europe on 28 January 1981 in Strasbourg, on the occasion of the third part of the 32nd Session of the Consultative Assembly.
4 As a result of the concerns about the ‘unjustified obstacles’ to the free flow of personal data across national borders is expressed in the OECD Guidelines, 1. The OECD Guidelines make it clear that privacy was
led to concerted action both nationally and internationally to provide a set of principles for the protection of personal information within member states and transmitted across borders.\(^5\) There emerged a general consensus on a common set of fair information practices whose purpose was to provide a balance between privacy protection and economic efficiency. The 1980 OECD Guidelines were developed to help harmonise national privacy legislation, to prevent disruptions in international flows of data, and to uphold human rights.

In relation to the EU, there are three institutions involved in EU legislation. These are the European Parliament, the Council of the European Union, and the EC.\(^6\) The EC is empowered to pass Directives that are binding on all Member States. Like the OECD, the Council of Europe feared that without a common code of conduct, different regulatory regimes might become a restraint on trade.\(^7\) The first half of 1990s was spent debating what regulatory mechanisms could ensure uniform application of ‘fair information practices’. The EU eventually established the requirements for ‘fair information practices’ in the form of the EC’s Directive 95/46/EC which came into effect in October 1998. The EC’s Directive 95/46/EC is binding on all EU Member States. Each EU Member State is required to pass legislation enacting the Directive into domestic law, and to establish an independent supervisory authority or data protection body with responsibility for its implementation. EU Member States are required to facilitate cross-border flows of personal data; protect the rights and freedoms of individuals, notably the right to privacy, with regard to the processing of personal data; and to harmonize laws and to enact laws

\(^5\) The transborder flows of personal information are governed by the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (hereafter referred to as the 1980 OECD Guidelines); See also OECD, ‘Recommendations of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (23 September1980).

\(^6\) The European Parliament works together with the Council representing national governments to decide on the content of EU laws and officially adopt them. The European Commission has one representative from each of the EU member states. It upholds the interests of the EU as a whole, and draft proposals for new European laws <http://europa.eu/about-eu/institutions-bodies/>.

\(^7\) For details on the history of privacy legislation refers to David H Flaherty, Privacy and Data Protection: An International Bibliography (Mansell, 1984); Colin Bennett, Regulating Privacy: Data Protection and Public Policy in Europe and the United States (Cornell University Press, 1992).
governing the processing of personal data’ to remove obstacles to the flows of personal data.\(^8\)

The key EC Directives such as the Council of Europe’s 1981 Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (Convention 108), and in particular Directive 95/46/EC establish norms of conduct in relation to information privacy in EU Member States and arguably non-member nations as a result of its transborder provisions. These will be discussed in detail below at [5.3.2.6].

The OECD Guidelines\(^9\) are non-binding on OECD members\(^10\) but rely on persuasion and consensus.\(^11\) The Guidelines expressly permit Member countries to ‘exercise discretion with respect to the degree of stringency with which the Guidelines are to be implemented’.\(^12\) Some countries have passed laws that apply to either only public sector or only the private sector as it was commonly perceived that only government agencies pose danger to individual privacy interests, and that the natural processes would limit the intrusiveness of corporations.\(^13\) All OECD member countries including the U.S., Australia,\(^14\) and New Zealand have endorsed the 1980 OECD guidelines with national information privacy protection laws based upon the OECD’s Guidelines.\(^15\) As shown in chapter 6 at [6.2.2] the OECD Guidelines have been modified by the Australian Privacy legislation.\(^16\) The OECD guidelines and EC’s Directives provide a comparative basis for examination of the Australian statutory provisions.

### 5.2 Information Privacy Protection – the OECD Guidelines

With the development of automatic data processing, the creation of international data banks and the ability to transmit personal data within seconds across national borders, this created an urgent need for legislation protecting privacy. The OECD introduced guidelines

---

8. See Directive 95/46/EC, Preamble, and Recitals 6-8 in Appendix 2.
9. A summary of the extract of the OECD Guidelines is reproduced in Appendix 1.
11. Ibid.
12. See 1980 OECD Guidelines, above n 5, Explanatory Memorandum 45, Guideline 2 and EM 43, Guideline 3(b), Guideline 4 and EM 46-47, Guideline 19 (g) and EM 52, 58, 59; Guidelines pt 4 [19 (b)] and Explanatory Memorandum [70].
13. The Australian legislation originally only applied to the government sector but was later extended to the private sector, see chapter 6 [6.2]. See also Roger Clarke, above n 4.
15. Ibid.
16. See Privacy Act 1988 (Cth) sch 3 NPPs in Appendix 3.
to prevent what it considered to be a violation of fundamental human rights. Privacy violations included the unlawful and in accurate storage of personal data, or the abuse or unauthorised disclosure of such data.\textsuperscript{17}

The OECD guidelines recommended privacy regulation in its member countries.\textsuperscript{18} An extract of the OECD Guidelines is provided in Appendix 1. By the early 1980s, approximately half of the OECD Member countries had introduced legislation broadly in line with the OECD Guidelines. The OECD Guidelines and recommendations by the OECD for consumer protection such as the Recommendation for the OECD Council Concerning Guidelines for Consumer Protection in the Context of Electronic Commerce,\textsuperscript{19} are designed to: provide ‘data protection’; reflect existing legal protection available to consumers in traditional forms of commerce; encourage private sector initiatives and consumer representation; and emphasise the need for co-operation between government, businesses and consumers.

The four main underpinning principles of the 1980 OECD Guidelines are: 1) the need to ensure free flow of information; 2) the avoidance of unjustified restriction on free flow of information resulting from domestic privacy legislation; 3) the necessity to guarantee basic rights of privacy as with respect to personal data; and 4) the need to harmonise the provisions of the various national laws.\textsuperscript{20} The OECD in 1980 adopted what are commonly referred to as ‘fair information practices’ (hereafter referred to as ‘FIPs’)\textsuperscript{21} which apply to the collection, processing, and use of ‘personal data’ whether by the public or private sector.\textsuperscript{22}

The OECD Guidelines cover the successive stages of the cycle that begins with the collection of data and ends with the erasure of data or similar measures. The Guidelines set limits to the collection of personal data, restrict usage and/or disclosure of data to conform with the specified purpose for which the data was primarily collected; create facilities for

\textsuperscript{17} See 1980 OECD Guidelines, above n 5, Preface.
\textsuperscript{18} The OECD Guidelines constitute a complementary safeguard to the International Telecommunications Convention of Malaga-Torremolinos, (25 October 1973).
\textsuperscript{20} See 1980 OECD Guidelines, above n 5, Preface, pt 4 [19]-[20].
\textsuperscript{21} For more details of the FIPs refer to the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data available at <http://www.oecd.org>. An extract of the eight fair information practice principles is provided in Appendix 2.
\textsuperscript{22} See 1980 OECD Guidelines, above n 5, Annex to the Recommendation, Scope of Guidelines [2], Explanatory Memorandum [40].
individuals to learn about the existence and contents of data and facilitate correction in the case of error; and the identification of parties who are responsible for compliance with the relevant privacy protection rules and regulation under national laws that give effect to the OECD principles. The Guidelines provide for the right to redress and there are explicit requirements to ‘provide for adequate sanctions and remedies in case of failure to comply’. The Australian National Privacy Principles (hereafter referred to as ‘NPPs’), with some modifications, are modelled on the OECD guidelines.

5.2.1 The Basic OECD Principles of National Application

The eight core principles comprise the following:

(1) Collection Limitation

Under the Collection Limitation principle there should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

(2) Data Quality

Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up to-date.

(3) Purpose Specification

The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

(4) Use Limitation

Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the purpose specification principle (see Explanatory Memorandum Para. 9 and 52) except: (a) with the consent of the data subject; or (b) by the authority of law.

23 See 1980 OECD Guidelines, above n 5, pt 4 [19(d)].
(5) Security Safeguards

Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

(6) Openness

There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

(6) Individual Participation

An individual should have the right:

a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;

b) to have communicated to him, data relating to him

- within a reasonable time;
- at a charge, if any, that is not excessive;
- in a reasonable manner; and
- in a form that is readily intelligible to him;

c) to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and

d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

(7) Accountability

A data controller should be accountable for complying with measures which give effect to the principles stated above. 24

---

24 See 1980 OECD Guidelines, above n 5, pt B, General Comments; Explanatory Memorandum [7]–[14].
It is not proposed to discuss every aspect of these eight core OECD principles but rather to draw out those elements which will be important for the discussion of the limitations of the Australian privacy legislation in chapter 6. The discussion deals with the following aspects: (1) Data Controllers; (2) Personal Data; (3) Openness and Participation; (4) Openness and Purpose Specification; and (5) Transborder data flows and accountability.

5.2.1.1 Data Controllers

A data controller is defined as a party who is legally competent to decide about the contents and use of data, regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf.25 The Guidelines impose obligations on controllers of personal data rather than just collectors of personal data. This has much in common with the EU provision which likewise imposes obligations on those making decisions about personal data. This approach has the benefit that it imposes responsibility on the decision maker rather than the persons who process data although in some instances both may qualify as data controllers. There are two limitations in relation to data controllers. The first is that the Guidelines do not necessarily apply to all actors who may handle or deal with personal data. The provisions only apply to parties who make decisions concerning the use, application and disclosure of personal information. The second is that OECD Guidelines apply only to organisations (data collectors) as defined. Of particular importance is the exemption in favour of those data controllers26 such as licensing authorities, data processing service bureaux carrying out data processing on behalf of others; telecommunications authorities and similar bodies acting as mere conduits, and ‘dependent users’ who may have access but not are authorised to decide what data should be stored or who should be able to use them, etc.27

The exemptions and exceptions28 allow collectors to use personal information for secondary purposes and provide opportunities for data mining (see chapter 2 at [2.2.2]). Individuals are exposed to increased potential harms as the value of personal data increases.

25 Ibid, Detailed Comments in General Definition Section, Explanatory Memorandum [1].
26 Ibid, Explanatory Memorandum [2], [3 (b)], [4]; Explanatory Memorandum [19 (g)], [40], [43], [45]-[47], [52], [58]-[59].
27 Ibid, Explanatory Memorandum [40].
28 Ibid, Explanatory Memorandum [19 (g)], [43] – [47], [58]–[59]. Explanatory Memorandum [45] expressly provides that Member countries can exercise their discretion as to the degree of stringency with which the Guidelines are to be implemented. Some countries such as Australia have enacted statutes exempting the private sector from compliance with the Privacy Act 1988 (Cth) until 2001, when the Act was amended to include the private sector organisations. There various exemptions for private sector data collectors such as individuals, small businesses, political parties, and the media. These are examined in detail in chapter 6.
the risks that personal data will be used in ways that the drafters of the OECD Guidelines had not anticipated. As previously discussed in chapter 2, the combination of various methods of data collection and processing of data allows far more detailed monitoring of an individual’s activities.

These exemptions give preference to corporate economic interests over that of the individual’s right to privacy and conflict with the Recitals to the OECD Guidelines which purport to give primacy to the privacy interests of data subjects. It contrasts with a much more protective regime under the EU referred to below at [5.3.2.1]. A similar issue of exemptions is raised in relation to the Australian legislation (see chapter 6 at [6.2.1], [6.2.1.2]).

5.2.1.2 Personal Data

The obligations imposed on data controllers apply to ‘personal data’ which is defined as ‘any information relating to an identified or identifiable individual (data subject)’. The provision interpreted broadly restricts the collection, disclosure and use of information if the individual is identifiable. The definition is important because, unlike the Australian provision (see chapter 6 at [6.2.1.3]), it is sufficient if the individual is identifiable with no qualification that the individual be reasonably identifiable which brings into account efficiency and cost issues.

29 The OECD Guidelines purport to give effect to art 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms. Article 8 – Right to respect for private and family life provides that, 1) Everyone has the right to respect for his private and family life, his home and his correspondence; and 2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

30 See the Annex to the OECD Guidelines and General Definitions; Directive 95/46/EC art 2 defines personal data as ‘any information relating to an identified or identifiable person (‘data subject’); an identifiable person is one who can be identified directly or indirectly, in particular by reference to an identifiable number or to one or more factors specific to his physical, psychological, mental, economic, cultural or social identity’. In contrast, the Privacy Act 1988 (Cth) uses the term ‘personal information’ and makes a distinction between ‘personal information and sensitive information. Privacy Act 1988 (Cth), s 6 defines personal information as, ‘information or an opinion (including information or an opinion forming part of a data base), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion’ And ‘sensitive information’ as, ‘any information regarding race, gender, political opinion, religious beliefs, philosophical beliefs, membership of a trade union or professional organisation, or sexual preference or practices.’ Chapter 6 at [6.2.1.3] discusses in detail the problem of inconsistency between the definition of ‘personal data’ and ‘personal information’, and ‘sensitive information’; See 1980 OECD Guidelines, above n 5, Scope of Guidelines [2], [3], [3 (c)]; Roger Clarke, ‘Beyond the OECD Guidelines: Privacy Protection for the 21st Century’ (1999) 18.
5.2.1.3 Openness and Participation

The Guidelines incorporate Openness and Individual Participation Principles. These require data controllers to provide and display adequate information about developments, practices and policies relating to personal data.\(^{31}\) The Guidelines impose obligations to provide data subjects the right to: obtain from a data controller confirmation of whether or not the data controller has data relating to the e-commerce user; a right to challenge the data relating to the data subject; and if the challenge is successful to have the data erased, rectified, completed or amended. A data controller is accountable for complying with measures which give effect to the principles stated above.\(^{32}\) The accountability principle is discussed below at [5.2.1.5]. Similar access and correction rights exist under the Australian provisions (see chapter 6 at [6.2.2.3]).

5.2.1.4 Openness and Purpose Specification

Under the Guidelines (the purpose specification principle) personal data cannot be:

… disclosed, made available or otherwise used for purposes other than those specified,\(^{33}\) and …the purposes for which personal data are collected should be specified not later that the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.\(^{34}\)

Under the purpose specification and openness principles, the primary purpose of the collection must be clearly understood by the consumer and identified at the time of the collection and expressly consented to.\(^{35}\) Consent is defined to mean ‘actual knowledge and consent’ of the ‘data subject’.\(^{36}\) The data subject’s consent must be obtained prior to personal data collection.\(^ {37}\) This is to ensure to the greatest possible extent that the

---

\(^{31}\) E-commerce users must have easy access to information concerning personal data held by the controller, how that information is used, the main purposes for which it is used as well as the identity and usual residence of the data controller.

\(^{32}\) See 1980 OECD Guideline, above n 5, Accountability Principles. The Accountability Principles aims to ensure that accountability is supported by legal sanctions. See 1980 OECD Guidelines, above n 5, pt B - General Comments, General Paragraph [7]-[14], Explanatory Memorandum [62].

\(^{33}\) Ibid, 1980 OECD Guideline, above n 5, Annex to Recommendations, Explanatory Memorandum [7]-[14].

\(^{34}\) Ibid, 1980 OECD Guideline, above n 5, Explanatory Memorandum [9].

\(^{35}\) For example if the primary purpose of the collection of transactional information is to permit a payment to be made for credit card purposes, then using the information for other purposes, such as data mining, without having identified this purpose before or at the time of the collection is in violation of these principles.

\(^{36}\) See 1980 OECD Guidelines, above n 5, Detailed Comments [41].

individual is aware of the collection and use of personal data so that the individual maintains control over the use and disclosure of his or her personal information. The EC provision similarly requires prior registration and consent, see Directive 95/46/EC arts 2 and 5 and discussion below at [5.3.2.1]). In contrast under the Australian Privacy Act principles, this principle is qualified as data collection, use and disclosure can occur without prior knowledge and consent if it is not practicable to obtain consent prior to its collection, use and/or disclosure with the rider that consent needs to be obtained as soon as practicable. This qualification gives preference to commercial interests over e-commerce users’ rights to privacy.

5.2.1.5 The Accountability Principle

Responsibility for ensuring that the Guidelines are complied with lies with a data controller. Under the OECD’s Accountability Principle, a data controller (as defined) remains responsible for complying with measures that give effect to the OECD principles even if data is transferred and processed in another jurisdiction. Under the accountability approach, obligations are imposed on those who make decisions about data; this can include data collectors, data processors, and third party beneficiaries to whom data is transferred. A data controller needs to ensure that personal information transferred across international borders is protected against unauthorised access, disclosure, modification or...

38 Ibid, Explanatory Memorandum - Introduction, cl 5 identifies that the core principles aim to protect privacy and individual liberties. The core principles set limits to the collection of personal data, restrict usage of data, to conform within openly specified purposes, create facilities for individuals to learn about the existence and contents of data, facilitate to have data corrected; and the identification of parties who are responsible for compliance with the relevant privacy protection rules and decision. These core principles cover the successive stages of the cycle that begins with the collection of data and end with the erasure of data or similar measures to ensure to the greatest possible extent for individual awareness, participation, and control over their personal data. It also provides that national laws should provide the greatest possible extent of individual awareness and participation and control. See 1980 OECD Guidelines: Explanatory Memorandum - Activities at National Level [5].

39 Although it should be noted that under current proposals, this requirement may change, see below at [5.3.2.3].

40 Privacy Act, NPP1 Collection, NPP2 Use and disclosure principle, see chapter 6 [6.2.2.1], [6.2.2.2]. See 1980 OECD Guidelines, Purpose Specification Principle [9] and Collection Limitation Principle (data collection methods) [10] in Appendix 1; see also Privacy Act NPP1.3 and NPP2 in Appendix 3; see also chapter 6 [6.2.2.1], [6.2.2.2].

41 See OECD Guidelines, above n 5, Accountability Principle, Explanatory Memorandum [14].


There are particular risks where data is transferred across borders. Typically these risks occur where there is outsourcing of customer data to overseas business processing centres that include sensitive personal data such as credit card applications, bills, mortgage applications, insurance claims and help desk services.

The OECD’s accountability approach appears to provide strong protection to e-commerce users where information is transferred to other organisations or across borders. A controller of information remains responsible for breaches of the guidelines. But the accountability principle is only as strong as the enforcement and compliance regimes of the individual country. Although there is recognition that controllers of personal data should demonstrate commitment to accountability by implementing data privacy policies, and mechanisms to ensure e-management and protection of personal data, the Guidelines are silent on, (1) what will be expected of companies in an accountability system, (2) how will enforcement agencies monitor and measure accountability, and (3) how can the protection of individuals be ensured.

If there are no clear guidelines, then this causes difficulties in achieving compliance, enforcement, and remedies for invasion of privacy. The EU takes a quite different approach which incorporates mechanisms for enforcement by its citizens where data is held or processed outside the EU.

In Australia the OECD principles have been adopted and form the basis of the Information Privacy Principles for the public sector and the National Privacy Principles (NPPs) for the private sector. As will be seen in chapter 6, the Australian provisions do not adopt an accountability principle so that privacy protection for Australian e-commerce users is substantially weaker than the OECD Guideline principles.

---

48 Martin E Abrams, above n 43, 2.
49 Ibid.
50 NPP9 governs transborder data flows out of Australia; see chapter 6 [6.2.2.5].
The mandated approach under Directive 95/46/EC appears to be stronger than the OECD Guidelines.\(^{51}\) Directive 95/46/EC arts 25 and 26 provide that personal data must only be transferred to if the host nation has adequate privacy laws that are equivalent to those in EU Member States. And if not then under art 26(2), the processor must be legally bound by contract or other legal act which requires the processor must only act on the controller’s instructions; employ staff bound by confidentiality; evaluate the risks to personal data and implement appropriate security measures to protect the data, art 30; and enter into an agreement with the controller to enable the exercise by data subjects of their rights under the regulation. This is discussed below at [5.3.2].

### 5.2.16 Summary

The above eight OECD Guideline Principles are important steps in the protection of information privacy. The limitations of the Guidelines are important to the Australian situation as the OECD Guidelines have largely been adopted with some modifications in Australian privacy laws (see chapter 6 at [6.2]).\(^{52}\) The OECD Guidelines are to be compared with the much stronger compliance regime established under the EU directives.

### 5.3 European Commission (EC) Directives

#### 5.3.1 Introduction

As noted previously all EU Member States are bound by the EC’s Directive 95/46/EC and required to pass legislation enacting the Directive into domestic law.\(^{53}\) Although the Directive aims to provide harmonised principles, there has been significant variation in implementation and interpretation between the member states. To overcome this there are currently proposals to create a single set of rules binding all member states and a single data protection authority; a one stop shop for enforcement and protection.\(^{54}\) The process to

---

52 See Privacy Act 1988 (Cth) sch 3 NPPs in Appendix 3.
54 See European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation, 2012/0011 (COD) Brussels 25 January 2012.
modernise Convention 108 began in January 2012. The objectives of the modernisation process were to deal with the challenges for privacy resulting from the use of new Information and Communications Technologies (ICTs), and to strengthen the Convention’s follow-up mechanism. These will be discussed below at [5.3.2].

Besides the EC’s Directive 95/46/EC, there are other EU privacy protection laws that are relevant to e-commerce. These include the Regulation (EC) No. 45/2001 of the European Parliament and the Council of 18 December 2000 on the Protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (hereafter referred to as Regulation 45/2001/EC); 57 Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (notified under document C(2010) 593) (hereafter referred to as Commission Decision 2010/87/EU); and Commission Decision 2002/16/EC of 27 December 2001 on standard contractual clauses for the transfer of personal data to processes established in third countries (hereafter referred to as ‘Commission Decision2002/16/EC’). 58 These EC Decisions and Regulations will be further discussed where relevant and appropriate in the following sections.


56 See European Commission, above n 55, Proposed Article 1 - Object and purpose.

57 Regulation 45/2001/EU art 2 not only requires a full-fledged system of protection of personal data but requires that Community institutions establish rights for data subjects and obligations for those who process personal data. It provides that appropriate sanctions for offenders and monitoring by an independent supervisory body. In addition Article 5 further provide that regulation must provide individuals with legally enforceable rights, to specify that the data processing obligations of the controller within the Community institutions and bodies to create an independent supervisory authority responsible for monitoring the processing of personal data by the Community institutions and bodies.

58 European Commission, Commission Decision 2010/87/EU art 6 refers to Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (notified under document c (2010) 593 (Text with EEA relevance) (2010/87/EU) (Commission Decision 2002/16/EC). Commission Decision 2002/16/EC, is relevant to the transfer of personal data to a third country that has inadequate level of data protection. It provides that if a processor established in a third country in adopts EU Member State’ laws which comply with the other provisions of the EC Directive 95/46/EC, are respected prior to the transfer, then Commission Decision 2002/16/EC provides that the prohibition under Directive 95/46/EC, OJ L 6, 10.1.2001 ‘may be lifted as soon as the reasons for the suspension or prohibition no longer exist’. See also Commission Decision 2002/16/EU art 4 (1) - (2).
The Directives crucially recognise privacy as a human right. In its preamble, Convention 108 underlines the human rights based approach of the Convention and emphasises that the major objective of the Convention is to put individuals in control of their personal data as a requirement for protection of human dignity. The proposed amendment to the current preamble to Convention 108 strengthens the commitment to privacy as a human right and recognises that rights to privacy take precedence over commercial interests. It provides that:

Considering that it is necessary, given the diversification and intensification of processing and exchange of personal data, to guarantee human dignity and the protection of human rights and fundamental freedoms of every person, in particular through the right to control one’s own data and the use made of such data;

Reminding (sic) that the right to protection of personal data is to be considered in respect of its role in society and that it has to be reconciled with other human rights and fundamental freedoms, including freedom of expression;

Considering that this Convention permits account to be taken, in the implementation of the rules laid down therein, of the principle of the right of access to public documents;

59 The Directive has as one of its objectives the recognition of basic fundamental rights recognised in the constitution and laws of Member States and in the European Convention for the Protection of Human Rights and Fundamental Freedoms. See the General provisions in the Recitals to EC Directive 95/46/EC Recital 1 – 3. EC Directive 95/46/EC Recital 10 provides that the general principles of European Community law must not result in any lessening of the protection afforded to an individual but seek to ensure a high level of protection in the European Community <http://www.cdt.org/privacy/eudirective/EU_Directive_.html>. In addition, the EC Directive provides that national laws must not lessen the protection afforded under Article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms. The Convention for the Protection of Human Rights and Fundamental Freedoms 1950 art 10 – Freedom of Expression provides that: ‘1) Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises; and 2) The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary’. Convention for the Protection of Human Rights and Fundamental Freedoms 1950 as amended by Protocols No. 11 and No. 14, art 8 Right to respect for private and family life provides that: 1). ‘Everyone has the right to respect for his private and family life, his home and his correspondence’; and 2). ‘There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others’.
Recognising that it is necessary to promote at the global level the fundamental values of respect for privacy and protection of personal data, thereby contributing to the free flow of information between peoples;

Recognising the interest of a reinforcement of international cooperation between the Parties to the Convention.  

As will be seen in the discussion of the current Directive 95/46/EC, the recognition of privacy as a human right gives preference to an e-commerce user’s right to privacy unless there is a compelling reason for overriding that right. In comparison, the Australian privacy legislation and related national privacy principles give preference to economic interests over individual privacy (see chapter 6 at [6.2.2]).

As previously noted although there are a number of other instruments that may be relevant, in this chapter the emphasis is on the most important and relevant to e-commerce and automatic processing of data, Directive 95/46/EC to which we now turn.

5.3.2 Directive 95/46/EC

The discussion following does not examine every aspect of the Directive but rather those aspects which reflect the priority given to individual rights of privacy over commercial interests particularly where the Australian legislation takes a different approach. It notes where relevant the current proposals for reform of the EU’s data privacy directives. It considers the application of the current Directive under the following headings: (1) Data controllers; (2) ‘personal data’; (3) Mandatory notification and consent prior to data processing; (4) Rights to access and correct data; (5) Data security and data security breach notification; (6) Transborder data flows; (7) The Right to Redress.


5.3.2.1 Data Controllers

The Directive imposes responsibility on data controllers. The Directive’s article (hereafter referred to as ‘art/s’) 2 (6), defines a controller as:

…the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purpose and means of the processing of personal data; where the purpose and means of processing is determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designed by national or Community law. 62

The definition is critical because the data controller remains accountable for compliance with the Directive with responsibilities to ensure data security, and the protection against improper usage, access or disclosure. Under the proposed EU’s data privacy reforms,63 the responsibilities of the data controller are expressly stated; a data controller would have the following obligations:

- Maintaining documentation relating to all processing operations for which it is responsible; the documentation must be made available on request by the supervisory authority (art 28)
- Responsibility for taking measures to ensure data security (art 30). This also extends to a processor (art 26)
- Where there are particular risks to the data subject’s human rights, a duty to undertake an assessment of the impact of the proposed processing on the protection of personal data (art 33).
- A duty to obtain authorisation from the supervisory authority before processing personal data to ensure compliance with the Regulation particularly in cases where there is data transfer to a third country or an international organisation (art 34). 64

---

62 A processor might also qualify as a joint controller. Directive 95/46/EC art 2(4) defines ‘processing’ as ‘any operation or set of operations which are performed upon personal data, including by automatic means or not such as collection, recording, organising, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction’. A processor is defined in art 2(5) as ‘a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller’.


64 There is a duty to consult where there are special risks under article 33.
- Appointing an independent data protection officer (art 35). In relation to private enterprises, this applies only where processing is carried out by an enterprise employing 250 or more persons.

The proposed reforms recognise that for comprehensive protection of information privacy, some obligations should be imposed not only on data controllers but also on processors to ensure compliance. The first step is that a data controller, who uses a processor to process information, is required to select a suitable processor who can give appropriate guarantees for compliance (art 26(1)). Secondly, under art 26(2), the processor must be legally bound by contract or other legal act which requires the processor must act only on the controller’s instructions; employ staff bound by confidentiality; evaluate the risks to personal data and implement appropriate security measures to protect the data, (art 30); and enter into an agreement with the controller to enable the exercise by data subjects of their rights under the regulation. This contrasts with the relatively weak accountability, compliance and enforcement under the Privacy Act and related National Privacy Principles in relation to the collection use and disclosure and the transborder transfer of personal information. This is discussed in chapter 6 at [6.2.2].

In addition to the adequacy principle under Directive 95/46/EC art 25 (see below in at [5.3.2.6]), the new EU proposals adopt an accountability principle under which data controllers would be required to put in place ‘appropriate and effective measures’ and to verify compliance with the Directive. This is important in the context of Australian laws which have a much more limited application to organisations leaving gaps in protection of individual privacy (see chapter 6 at [6.2.2.5.3]).

Under the Directive there are very limited exceptions. Under art 3, the Directive does not apply to the processing of personal data: if it is in the course of an activity which falls outside the scope of European Community law; or if the processing operation concerns public security, defence, State security (including the economic wellbeing of the State, and

---

65 The position and duties of the data protection officer are set out in arts 36, 37.
66 It also applies where systematic monitoring is required which is less likely with a private business. See Council of Europe, Modernisation of Convention 108 (17 September 2012), art 35(1) (c).
67 Note the extended definition of processing in art 4(3).
in areas of State’s criminal law; or activities by individual persons in the course of a purely personal or household activity. It is important to note that exemptions are limited to public interest exceptions. This is an important as it gives preference to the e-commerce user’s right of privacy over and above commercial interests. In contrast under the OECD Guidelines (above) and under Australian Privacy legislation, there are significant exceptions giving preference to commercial interests and efficiency. In Australia, the most important exemptions are small business and transfer between related companies (see chapter 6 at [6.2.1.2]).

5.3.2.2 Personal Data

Directive 95/46/EC applies to personal data which is defined in art 2(1) as,

...any information relating to an identified or identifiable person (‘data subject’); an identifiable person is one who can be identified directly or indirectly, in particular by reference to an identifiable number or to one or more factors specific to his physical, psychological, mental, economic, cultural or social identity.  

It goes on to define an ‘identifiable person’ in art 2(2) as,

...one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, psychological, mental, economic, cultural or social identity.  

The protection applies whether the person can be identified directly or indirectly. A proposed change to the Directive adds the qualification that an individual is not considered as being identifiable if it would require ‘unreasonable time or effort for the controller or for any person from whom the controller could reasonably obtain the identification’.  

69 See Directive 95/46/EC art 2. In contrast, the Privacy Act 1988 (Cth) uses the term ‘personal information’ and makes a distinction between ‘personal information and sensitive information. Privacy Act 1988 (Cth) s 6 defines personal information as, ‘information or an opinion (including information or an opinion forming part of a data base), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion’ And ‘sensitive information’ as, ‘any information regarding race, gender, political opinion, religious beliefs, philosophical beliefs, membership of a trade union or professional organisation, or sexual preference or practices.’ Chapter 6 at [6.2.1.3] discusses in detail the problem of inconsistency between the definition of ‘personal data’ and ‘personal information’, and ‘sensitive information’.

70 It does not apply to data where the data subject is no longer identifiable (see Recital 26). There are further provisions relating to the storage of identifiable data, see art 6.

71 Additionally under the proposal ‘identifiable’ extends to ‘what allows the individualising of one person amongst others’. See Council of Europe, ‘Proposal for the Modernisation of Convention 108’ (27 April
although the test of identification appears to be qualified, unlike the Australian provisions (see chapter 6 [6.2.1.3]), the onus is on the data controller to show that identification is not possible without unreasonable expenditure of time and effort.

The working paper on the proposed reform of the EU’s Privacy directive also suggests that one option promoting increased responsibility is for the Directive to explicitly refer to online identifiers as personal data. The recommended art 20 would effectively prevent certain types of profiling based on these online identifiers. These reforms address some of the limitations in defining ‘personal data’. The Australian privacy legislation is much more restrictive; online identifiers may not qualify as personal information, moreover personal data is only protected if the person can be identified or is ‘reasonably’ ascertainable; this brings into play issues of cost and efficiency (see chapter 6 [6.2.1.3]).

5.3.2.3 Mandatory Notification and Informed Consent Prior to Data Processing

Subject to exemptions, Directive 95/46/EC arts 18-21 requires mandatory notification to the relevant supervisory authority prior to any automatic data processing operations (see art 18). The notification must specify the name and address of the data controller; the purpose of processing, a description of the categories of data, the recipient or categories of recipient to whom the data might be disclosed, and proposed transfers of data to third countries (see art 19). Member states are also required to determine if the processing operations are likely to pose specific risks to the rights and freedoms of data subjects (see art 20), and to check those operations prior to their commencement as well as ensuring

---


73 Under Directive 95/46/EC art 18 (2), Member States may provide for the simplification of or exemption from notification in cases where categories of processing operations are unlikely to affect adversely the rights and freedoms of data subjects, or if the controller specifies the purpose of processing; or if it is in compliance with national law. There is considerable variability in exemptions among Member States, for example, some exempt where a Data Protection Officer has been appointed, see European Commission, ‘Commission Staff Working Paper Impact Assessment’, Brussels, 25 January 2012, 14.

74 Directive 95/46/EC art 8 provides that the controller or his representative, if any must notify the supervisory authority referred to in art 28, before carrying out any wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes.

75 Directive 95/46/EC art 19 provides for content of notification which include the name and address of the controller and of his representatives if any; the purpose or purposes of the processing; a description of the category or categories of data subject and of the data or categories of data relating to them; the recipients or categories of recipient to whom the data might be disclosed; the proposed transfer of data to third countries; a general description allowing a preliminary assessment to be made of processing.

76 Directive 95/46/EC art 20 provides that ‘the processing of data is carried out by a person established in a third country must not stand in the way of the protection of individuals provided for in this Directive;
that processing operations are publicised (see art 21). Current proposals recommend that instead of prior registration, there should be far greater emphasis on accountability on the part of the controller with the controller being required to adopt policies and implement appropriate measures to ensure and to demonstrate that there is compliance with the data protection rules. Under this recommendation the controller must be able to verify compliance.\textsuperscript{77}

Under the existing Directive 95/46/EC, in addition to the notification requirement, prior to personal data processing, art 7 requires the data subject give unambiguous consent to the processing of their personal data.\textsuperscript{78} Article 2 (h) defines ‘consent’ as,

\begin{quote}
any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.
\end{quote}

Some states have interpreted this to require express consent in writing others that some form of implied consent is sufficient.\textsuperscript{79} The 2012 reform proposals set up a uniform definition. In the proposed art 4(8), a data subject’s consent means,

\begin{quote}
…any freely give specific, informed and explicit indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed…
\end{quote}

The data subject under the proposed reform is also given a right to withdraw consent at any time, art 7(3). Under the proposed reforms, art 7(4) also recognise that in some situations a person giving consent may not be able to genuinely consent, for example, in

\begin{quote}
whereas in these cases, the processing should be governed by the law of the Member State in which the means used are located, and there should be guarantees to ensure that the rights and obligations provided for in this Directive are respected in practice’.
\end{quote}

\textsuperscript{77} See European Data Protection Supervisor, ‘Opinion of the European Data Protection Supervisor’ (7 March 2012) [166]-[170]. This is in contrast to the Australian position that does not provide for prior notification of data collection to the supervisory authority, see chapter 6 at [6.2.2].

\textsuperscript{78} Directive 95/46/EC art 7 provides that personal data may only be processed if: the data subject has unambiguously given this consent or if the processing is necessary for the performance of a contract to which the data subject is a party to or if it is in order to take steps at the request of the data subject prior to entering into a contract. Article 8 expressly prohibits the ‘processing’ of sensitive data that reveals a person’s racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and data concerning health and sex life. There are some limited exemptions under art 8. It may be processed where there is explicit consent, see art 3.

relation to employees. In those situations consent does not ‘provide the legal basis for processing’. These provisions promote the autonomous choice of the individual whether to consent to usage of personal data. It contrasts with the Australian provisions which are discussed in the chapter following (see chapter 6 at [6.2.2.1]). Even under the current EC Directive, the requirement of unambiguous consent provides greater protection than the Australian provisions where implied consent is frequently sufficient (see chapter 6 at [6.2.2.1.1], [6.2.2.2.1]).

Directive 95/46/EC art 10 provides that if a data controller (or the controller’s representative) collects information from a data subject, then at the time data is collected, the data controller or his representative must provide the data subject information such as:

- the identity of the controller and his representative; 80
- the intended purpose of the processing;
- information about the recipients or category of recipients of the data;
- whether replies to the questions are obligatory or voluntary and the possible consequences of failure to reply;
- the right to access to and the right to rectify the data concerning the data subject free of charge (see arts 12, 14); and
- to provide a guarantee fair processing of the personal data in respect of the data subject (see art 10). 81

If information about the data subject is not collected from the data subject then art 11 requires that the controller or his representative must the information as required under art 10. Under the 2012 reform proposals, in addition to the above requirements, the data subject must also be informed about the right to lodge a complaint and the contact details of the supervisory authority (see art 14(1) (e)) as well as whether it is intended to transfer

80 Under the proposed 2012 reforms information concerning the data protection officer is also required, (art 14(1) (a)). See European Commission, Proposals for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Brussels, 25 January 2012, COM(2012) 11 final 2012/0011 (COD).
81 Directive 95/46/EC art 10 provides for information to be given to the data subject in cases of collection of data from data subject)
data to a third country and the level of protection available in that third country (see art 14(1) (g)).

There is the further provision in art 14 which gives e-commerce users a right to object on legitimate grounds; to the processing of data relating to them without reasons, on request and free of charge. Under the proposed reforms, the e-commerce user is given the right to object to processing of personal data on limited grounds. It is up to the controller to demonstrate that there are ‘compelling legitimate grounds...which override the fundamental rights and freedoms of the data subject’ (see art 19(1)). Human rights are thus given priority over economic and commercial interests unless the data controller can justify the processing of that data. In relation to personal data to be used for direct marketing purposes, e-commerce users are given the right to opt out. Under the proposed reforms, art 19(2) state that this right to opt out must be explicitly offered in easily understood language and separately identified as an option.

The proposed reforms to Directive 95/46/EC add a very important protection, the right to erasure in the proposed art 17. In addition, the proposed art 18 creates a new right allowing data subjects to obtain a copy of their personal data undergoing processing in an electronic format and to transmit it from one electronic service provider to another. But it is unclear from the current text how the right to data portability under the proposed art 18 relates to the right to erasure and if data should be deleted by the data controller once the right has been invoked. This is because under the proposed article 5 (e) the data controller is required to delete data that is no longer necessary for the purpose for which the data is processed unless the data controller has a legal basis for continuing to process some of the

82 See European Commission, above n 80. The 2012 reform proposals set out some exceptions to prior notification of data collection in art 14(5) such as where the data subject already has the information referred to in art 10 of Directive 95/46/EC above; if the data is not collected from the data subject and the provisions of such information proves impossible; if it would involve a disproportionate effort; if the data are not collected from the data subject and recordings or disclosure is expressly laid down by law; if the data are not collected from the data subject and the provision of such information will impair the rights and freedoms of others, as defined in the Union law or Member State law in accordance with the proposed art 21. The proposed art 21 provides that Union or Member State law may restrict by way of legislative measures the scope of the obligations and rights.

83 The grounds set out in proposed art 6(d)-(f). Under art 6 (d) processing is necessary to protect the vital interests of the data subject; (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority (f) or protection of the controller’s legitimate interests except where these interests override the data subject’s fundamental rights and freedoms. The right to object does not extend to situations where consent has been given for one or more specific purposes (6(1) (a)) or necessary for performance of a contract with the data subject or compliance with a legal obligation, art 6(1) (b) (c).

84 See European Commission, Opinion of the European data Protection Supervisor on the Data Protection Reform Package, Brussels (7 March 2012) [146]-[149].
data for example to comply with legal obligations such as for tax purposes. So art 18 should clarify that the exercise of the right to portability is without prejudice to the obligation to delete data when they are no longer necessary according to art 5 (e).  

These are very important provisions as they provide protection for personal data that recognises an e-commerce user’s human right to privacy. Under the existing EC’s Directive, the notification to the supervisory authority prior to data processing allows monitoring of data collection, processing, usage and transfer of data. The Directive also recognises e-commerce users’ right of autonomy to make decisions about themselves and their lives. The proposed reforms clarify that e-commerce users can refuse to consent to collection of personal data and that consent must be explicit, unambiguous and sufficiently informed. This approach gives effect to e-commerce users’ right to privacy in relation to their personal information and recognises it as a human right not to be traded off against commercial interests. As will be seen when the Australian provisions are discussed, in Australia there is no requirement of prior notification to the supervisory authority; moreover in some circumstances information can be transferred, disclosed and used without the prior express consent of the e-commerce user (see chapter 6 at [6.2.2.1.1], [6.2.2.2]).

In summary, Directive 95/46/EC recognises e-commerce users’ individual rights to autonomy, to decide for themselves what is in their own best interests and consequently provides strong protection for privacy rights of e-commerce users. These rights are not subservient to commercial interests as it is argued is the case with the Australian legislation (see chapter 6 at [6.2.2]).

### 5.3.2.4 Rights to Access and Correct Data

Directive 95/46/EC also gives data subjects important rights such as access to data about them, information about where the data originated (if such information is available), the ability to rectify inaccurate data, and recourse in the event of unlawful processing of personal data which include withholding or withdrawing consent to the use of their data. In  

---

85 European Commission, Proposals for a Regulation of the European parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Brussels, 25 January 2012 COM(2012) 11 final 2012/0011 (COD). See also European Commission, above n 84, [150]-[152].
86 Directive 95/46/EC art 12 (a).
87 Directive 95/46/EC art 12 (b).
particular, Directive 95/46/EC art 12 requires member states to guarantee every data subject the right to obtain from the controller a confirmation as to whether or not data relating to him is being processed and information as to the purposes of the processing. It also provides for the appropriate rectification, erasure or blocking of data if the processing of which does not comply in particular because of the incomplete or inaccurate nature of the data; and notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with the EC’s Directive unless this proves impossible or involves a disproportionate effort. The proposed reforms provide additional protection with a right to have the material erased when it is no longer required. In short the ability to collect, use and disclose personal data is permitted only to the extent absolutely necessary. Any infringement of an e-commerce user’s right to privacy must be justified and only available where it is necessary. These rights will be compared with the rights of Australian e-commerce users to access and be given information on personal data relating to them (see chapter 6 [6.2.2.3]).

5.3.2.5 Data Security and Data Security Breach Notification

Directive 95/46/EC arts 16 and 17 provide for confidentiality and security of processing. Article 16, requires any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data not to process data except on instructions for the controller unless required to do so by law’. Article 17(1), provides that,

…the controller must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alternation, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Under Directive 95/46/EC art 17(2), the controller must provide sufficient guarantees in respect of the technical security measures and organisational measures governing the processing to be carried out as mentioned in art 17(1), and must ensure compliance with those measures. Article 17(3) provides that the carrying out of the processing must be governed by a contract or legal act binding the data processor to the controller; it must

88 Directive 95/46/EC art 17.
stipulate that the processor shall act only on instructions from the controller; and that the
obligations under art 17(1) discussed above are imposed on the processor. Article 17(4)
provides that the contract or legal act relating to data protection shall be in writing or in
other equivalent form. The proposed reforms impose a duty on the controller to notify the
supervisory authority within 24 hours where there is a data breach and following that
notification, notify the data subject if affected without undue delay (see art 32). A
processor has a duty to inform the controller of a personal data breach (see art 31(2)). The
controller is required to document the breaches and remedial action taken sufficient to
enable the supervisory authority to verify compliance (see art 31(4)).

It can be seen that Directive 95/46/EC sets out detailed legal obligations on the controller
and the processor to protect data security. In contrast, the Australian legislation does not
set in place legal structures to enhance data security and responsibility where the
organisation collecting the data is not necessarily the same as the processor or the
organisation making decisions about usage of the data (see chapter 6 at [6.2.2.5]).

5.3.2.6 Transborder Flows of Personal Data

Directive 95/46/EC also requires that personal data relating to European citizens be
protected by privacy standards deemed adequate when it is exported to, or processed in,
countries outside the EC, ‘third countries’. The EC’s adequacy approach is set out in art
25. Article 25 requires that the transfer of personal information to a third country may only
take place if the third country provides assurances of an adequate level of protection that is

---

89 But only if feasible with the onus on the data controller to show why notification was not made within 24
hours, article 31(1). The proposed regulation fails to specify the criteria and requirements for establishing a
data breach and the circumstances in which it should be notified; See EUR-Lex, ‘Safeguarding Privacy in a
Connected World: A European Data Protection Framework for the 21st Century’ (COM (2012) 9 final); see
also the European Data Protection Supervisor, Opinion of the European Data Protection Supervisor:
90 Directive 95/46/EC art 32.
91 Ibid, art 31.
92 See Australian Law Reform Commission, ‘For Your Information; Australian Privacy Law and Practice,
(‘Report 108’) (2008) [51.2].
93 See Directive 95/46/EC arts 23-25. The EC Directive also refers to rules of law, both general laws on the
protection of individuals as regards to the processing of personal data and sectoral laws such as those relating
to statistical institutes, (see EC Directive 95/46/EC art 23) in force in the third countries in question and the
professional rules and security measures which are complied with in those countries’.
94 There is special provision relating to transfers of data between related companies of multinational
corporations. Data transfers may take place to those related companies where there are approved Binding
Corporate Rules. Whilst these avoid a multiplicity of contractual arrangements for data transfer, there are
considerable difficulties where other member states have different or more onerous requirements, see pp16-
2012. The proposed reform extends to transfers to International Organisations (see art 40).
assessed on the basis of all circumstances including the rules of law, both general and sectoral that is in force in the third country in question. Article 25(2) sets out the criteria against which a foreign country’s privacy protection is assessed as follows:

... particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.

Not all jurisdictions to which data is transferred or processed have privacy laws or adequate privacy laws.95 Australia, for example, does not meet the adequacy standard most especially because of the exemptions from the Privacy Act such as small business (see chapter 6 at [6.2.1.2]).96 Jurisdictions where information privacy protection is deficient or provide less protection than those in EU member states are subject to data export limitations.97 Although the EC’s Directive 95/46/EC does not require the adoption of the same legislative arrangements by all countries through which personal data about European citizens flows, the Directive 95/46/EC places pressure on countries outside Europe to adopt privacy standards that meet European standards of adequacy. The EC Directive is especially important in establishing international norms. This is because it imposes obligations on member states and restricts transborder flows of information and permits the transfer of data to non-member states only where equivalent protection is available or other measures are taken. For example the EU framework for information privacy has impacted other countries that transfer personal data to a third country such as the U.S., and New Zealand.98 In this sense it sets international norms of conduct for information privacy.

In addition to Directive 95/46/EC art 25, there is the further provision which allows the transfer of information to a non-complying country if adequate safeguards are in place.

---

95 Directive 95/46/EC art 25(2).
96 The Privacy Act 1988 (Cth) does not impose an obligation on organisations to notify individuals whose personal information has been compromised. See Australian Law Reform Commission, above n 92 [51.2]. In contrast to art 25, the Privacy Act does not require explicit and unambiguous consent to collection or transfer of data; see Privacy Act 1988 (Cth) NPP9 – Transborder data flows in Appendix 3; See also Directive 95/46/EC art 7 on the criteria for making data processing legitimate and art 2 in respect to the definition of ‘consent’.
98 Directive 95/46/EC art 25. Article 25 restricts the transfer of personal information to countries that do not have equal, if not more stringent protection for personal information.
Directive 95/46/EC art 26 (1) provides that EU Member states may transfer personal data to a third country which does not have adequate level of protection within the meaning of art 25 if: (1) the data subject has unambiguously consented to the transfer, or (2) if the transfer is necessary for the performance of a contract between the data subject and the controller, or (3) the implementation of pre-contractual measures taken in response to the data subject’s request, or (4) for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party.  

Under art 26(4), the EC is empowered to decide on certain standard contractual clauses as providing sufficient safeguards as required under art 26(2).\(^{99}\) EC Decision 2002/16/EC (hereafter referred to as ‘Commission Decision 2002/16/EC’),\(^{100}\) under Directive 95/46/EC has been adopted to facilitate the transfer of data from a data controller established in the EU to a processor established in a third country which does not have adequate level of protection set under art 25. Since its adoption there has been increasing use of standard contractual clauses for the transfer of personal data to non-compliant third countries.\(^{101}\) The contractual obligations apply to the ‘data exporter’ and the ‘data importer’.\(^{102}\)

---

\(^{99}\) Directive 95/46/EC art 26. The adequacy principle is retained under the proposed Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General data Protection Regulation) COM(2012) 11 final 2012/0011 (COD), Brussels, 25 January 2012. Article 40 (General principle for transfer), provides that the transfer can take place only if the conditions for transfers set forth in the proposal Regulation are met. Article 40 also clarifies that the rules on transfer apply not only to controllers but also to processors and to any additional recipients in the case of onward transfers. The Commissioner’s power to adopt decisions recognising the adequacy or non-adequacy of a third country now also involves international organisations. In addition the proposed art 41 (Transfer with an adequacy decision), introduces a new criteria for the assessment that focuses clearly on the rule of law and the existence of effective redress mechanisms and of an independent supervisory authority in the third country in question. Self-regulation continues to be an option (see art 41 (2). The benefit is that the proposed Regulation provides some flexibility and sets up a new mechanism to be used to provide adequate safeguards for data transfers to third countries which do not benefit from an adequacy decision. The new mechanism includes a detailed mechanism for the use of and the conditions for the use of various types of contractual clauses that gives contractual clauses a clear legal basis in the Regulation. See European Data Protection Supervisor (EDPS), Opinion of the European Data Protection Supervisor on the Data Protection Reform Package, Transfer to Third Countries (Chapter V) [214]–[216].

\(^{100}\) The EU’s model contract clauses are available at <http://www.europa.eu.int/comm/internal_market/privacy/modelcontracts_en.htm>. Under the proposed reforms appropriate safeguards may be provided by: (a) binding corporate rules (art 43); standard data protection clauses adopted by the Commission or supervisory authority; contractual clauses between controller or processor and recipient of the data authorised by a supervisory authority, art 42(2). In relation to data where there is no legally binding instrument, prior authorisation is generally required, art 42(5).


\(^{102}\) See European Commission, Commission Decision 2010/87/EU, above n 101, [7].
parties to the contract can include any other clauses pertinent to a business related contract provided they do not contradict the standard contractual clause required under Commission Decision 2002/16/EC. In addition to Commission Decision 2002/16/EC, Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (notified under document C (2010) 593), (hereafter referred to as ‘Commission Decision 2010/87/EU’) sets out the clauses and the provision that the law of the EU applies.

By incorporating standard contractual clauses into a contract, the Council and the European Parliament aim to ensure that personal data can only flow from a data collector from EU Member States to a data collector established in a country that ensures and provides for an adequate level of data protection. Commission Decision 2010/87/EC at [19] provides that in the event of a breach, the standard contractual clauses should not only be enforceable by the organisations which are parties to the contract but also by the data subjects if data subjects suffer damages from a breach of contract.

The data subject should be entitled to take action and where appropriate receive compensation from the data exporter who is the data controller of the personal data transferred (see Commission Decision 2010/87/EC at [20]). Where there is a dispute between the data subject who invokes a third party beneficiary clause and the data importer that is not a country who agrees to receive from the data exporter personal data intended for processing on the data exporter’s behalf after the transfer in accordance with his instructions and the terms of this Decision and who is not subject to a third country’s system ensuring adequate protection within the meaning of Article 25 (1) of Directive 95/46/EC.’


Ibid, above n 101. Clause 4 provides that, standard contractual clauses should relate only to data protection. Therefore, the data exporter and the data importer are free to include any other clauses on business related issues which they consider as being pertinent for the contract as long as they do not contradict the standard contractual clauses’; cl 15 provides that ‘the data importer should process the transferred personal data only on behalf of the data exporter and in accordance with his instructions and the obligations contained in the clauses. In particular the data importer should not disclose the personal data to a third party without the prior written consent of the data exporter. The data exporter should instruct the data importer throughout the duration of the data-processing services to process the data in accordance with his instructions, the applicable data protection laws and the obligations contained in the clauses’.


European Commission, Commission Decision 2010/87/EU, above n 101, cl 22 provide that, ‘the contract should be governed by the law of the Member State in which the data exporter is established enabling a third-party beneficiary to enforce a contract. Data subjects should be allowed to be represented by associations or other bodies if they so wish and if authorised by national law. The same law should also govern the provisions on data protection of any contract with a sub-processor for the sub-processing of the processing activities of the personal data transferred by the data exporter to the data importer under the contractual clauses’.
amicably resolved, the data importer should offer the data subject a choice between mediation and litigation. Under Commission Decision 2010/87/EC at [22], the contract should be governed by the law of the Member State in which the data exporter is established enabling a third-party beneficiary to enforce a contract.

Under proposed reforms to Directive 95/46/EC, data may be transferred to a third country or an International organisation if, (a) there has been an ‘adequacy decision’ that the third country or organization provides adequate privacy protection (art 41), or (b) there are appropriate safeguards in place (art 42). Article 42 contemplates a range of options which will secure the privacy of data transferred out of the EU. These can include Binding Corporate Rules (art 43) and contractual clauses which protect privacy and provide remedies for breach, or (c) if neither apply, then under art 44 a transfer may take place if certain conditions are met. These include the consent of the data subject provided the data subject has been informed of the risks; transfer related to contractual performance; public interest, the exercise of defence of legal claims; the protection of interests of the data subject or another person where the data subject is incapable of giving consent; where the legitimate interests of the controller or processor are involved where appropriate safeguards are in place. Under art 44, the responsibilities attach to controllers as well as processors and to others involved in retransfer.

Although the current Directive 95/46/EC and decisions provide strong measures to ensure that the privacy of the e-commerce user is not compromised where data is transferred out of the EU, under the proposed reforms, even stronger measures are recommended. These impose responsibilities on both the data controller and processor. Measures taken must be ‘appropriate and effective’, and they must be documented and verifiable. The Australian legislation in comparison has very weak compliance and verification requirements, and duties are not imposed on organisations making the decisions about data nor are obligations directly imposed on data processors (see chapter 6 at [6.2.2.5]).

---

108 A list of adequate or inadequate provision is to be published in the Official Journal of the European Union, article 41(7).
109 European Data Protection Supervisor, above n 99, [215] - [216].
110 Ibid, [214].
5.3.2.7 The Right to Redress

Directive 95/46/EC has provided an added incentive for e-commerce providers to comply with privacy policies. If individual e-commerce users suffer damage as a result of the unlawful processing of data, they are entitled under Directive 95/46/EC to judicial remedies and compensation from the data controller. The Directive also sets up compliance and enforcement measures (see art 21). EU Member states are required to adopt suitable administrative, civil or criminal sanctions in compliance with Directive 95/46/EC arts 22-24. The EU has also provided a mechanism by which an individual whose privacy has been infringed can bring a private action for enforcement. Directive 95/46/EC art 28 provides that the supervisory authority is to have a wide range of powers that include investigative, intervention powers and the right to take legal proceedings for enforcement. In contrast, reflecting a much more pro-commerce stance, the Australian privacy legislation does not provide adequate remedies or enforcement to protect the individual e-commerce user where there has been a breach of her or his privacy. This is discussed further in chapter 8.

5.4 Conclusion

The OECD Guidelines and the EC’s Directives provide an important backdrop to the examination of the Australian privacy legislation. The Australian legislation is based on the OECD principles but with significant modification as will become apparent in the Chapter following. The OECD and EC provisions are important in their recognition of privacy as a human right. In this respect the EC provisions provide stronger recognition of privacy as a human right, particularly on the requirement of informed, unambiguous and explicit consent, opt out provisions for direct marketing, data security and breach notification as well as more protective provisions relating to transborder transfer and the provision of adequate remedies. The OECD principles, in some aspects, allow commercial

111 Directive 95/46/EC art 28-30 require Member States to provide in their national legislation for the establishment of a supervisory authority, and working party on the protection of individuals with regards to the processing of personal data.
112 The 1980 OECD Guidelines provides in its Preface that the reason OECD Member countries consider it necessary to develop Guidelines which would help to harmonize national privacy legislation and, while upholding such human rights, would at the same time prevent interruptions in international flows of data; and Directive 95/46/EC provides under [1]–[2] that fundamental rights and freedoms notably the right to privacy must be protected besides contributing to economic and social progress, trade expansion and the well-being of individuals.
interests to trump the e-commerce user’s right to privacy. This is particularly the case with exemptions from the OECD principles (see above at [5.2.1]).

The most important elements for the protection of information privacy include: consent to the collection of personal data, and control over the use and/or disclosure of personal information; the right to access and correct inaccurate information about the data subject and the proposed right to erasure and the right to forget; the transborder flow of personal information; and the security of that data. Subject to limited exceptions, the EC’s Directive restricts the trans-border flow of personal information outside the European Community if the third country does not have adequate laws to protect the personal data of EU citizens or if adequate safeguards are not in place,113 or if the consumer expressly consents.114 In contrast to the OECD Guidelines, it appears that the EU provision for privacy as a human right provides stronger protection to EU citizens not only within their own EU member countries but also externally through its restriction on the transfer of personal data. Both the OECD Guidelines, the EU aim to provide effective mechanisms for securing privacy. The OECD Guidelines are non-binding on Member States, while compliance with the EC’s Directives for EU Member States is binding. Although non-binding on countries outside the EU, the Directives have influenced privacy legislation in many countries including the U.S., New Zealand, and Australia.115 It can therefore be seen that the EC Directive 95/46/EC, in particular is very influential in achieving information privacy protection.116 What is crucial is that the EC’s Directive recognises privacy as a human right that is given preference over commercial interests.

The following chapter will examine the primary legislation for privacy protection in Australia, the Privacy Act. The chapter will highlight the differing OECD and EU provisions where the Australian legislation provides a lower level of protection for e-commerce users.

---

114 The other exceptions under art 26 (1 (a)–(f), (2) apply if the personal data is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken in response to the data subjects request.
115 For example countries such as the U.S., Australia, and New Zealand have passed privacy laws which are the Privacy Act 1974 (U.S.), the Australian Privacy Act 1988 (Cth), and the New Zealand Privacy Act 1993. 116 For a detail discussion refer to David H Flaherty, ‘Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States, (University of North Carolina Press, 1989) 306; Fred H Cate, ‘Privacy in the Information Age,’ (The Brookings Institution Press, 1997) 32, 220.
Chapter 6: Statutory Information Privacy Protection in Australia

6.1 Introduction

This chapter deals with Australia’s federal statutory framework for information privacy protection. As previously mentioned in chapter 1, this thesis is concerned only with statutory regulation at the federal level, principally, the Privacy Act 1988 (Cth) (hereafter referred to as ‘Privacy Act’) and the National Privacy Principles (hereafter referred to as ‘NPPs’).¹ The emphasis is on the statutory framework because although common law actions for breach of privacy may be available in NZ, U.S., and UK (based on an expanded duty of confidentiality), there is, as yet, no general right of privacy under Australian law.² The common law has not as yet developed a tort of privacy. Such protection as there is at common law in Australia is incidental to protection of property, contract, torts and equity claims, particularly the action for breach of confidence.³ Similarly, whilst the Australian Constitution may protect some incidental rights there is no express constitutional right to privacy in Australia.⁴

The sections following discuss the major provisions of the Privacy Act and the related NPPs. It will also make brief reference to overlapping legislation in the Telecommunications Act 1997 (Cth) (‘Telecommunications Act’),⁵ and the Spam Act 2003 (Cth) (‘Spam Act’).⁶

¹ Privacy Act NPPs are reproduced in Appendix 3.
³ Carolyn Sappideen and Prue Vines, ‘Fleming’s: The Law of Torts’ (Lawbook Co, 10th ed, 2011) [26.20]. Although a statutory tort for protection of privacy has been mooted, there has been no formal steps have been taken to legislate such a right.
⁴ However under the Commonwealth of Australian Constitution Act 1900, there is the individual’s right to be treated justly by the government when acquiring private property (s 52 (31); the right to trial by jury from serious criminal offences (s 80); the right to follow any religion (s116); and other rights such as free speech on political matters may be implied under the common law and constitutional powers. See Theophanous v The Herald Weekly Times Ltd (1994) 182 CLR 104. The High Court recognised an implied right under the Constitution to free speech on political matters. In 1997 the High Court in Lange v Australian Broadcasting Corporation (1997) 189 CLR 520 held that the implied right to free speech was only available ant could satisfy the tests of qualified privilege. The Commonwealth of Australian Constitution Act 1900 is available at <http://www.comlaw.gov.au>.
⁵ Hereafter referred to as the ‘Telecommunications Act’.
⁶ Hereafter referred to as the ‘Spam Act’.
6.2 Privacy Act and NPPs

The Privacy Act is the main federal legislation that protects personal information privacy in Australia. It was originally enacted in 1988 and applicable only to public agencies. The Act was subsequently amended in 2001 to apply to private sector organisations as well. The Privacy Act sets the minimum standards for protection of privacy for the public sector,\(^7\) and the private sector. Private sector standards are contained in the NPPs\(^8\) which are broadly based on the eight OECD Guidelines.\(^9\)

The Privacy Act and NPPs set out privacy obligations in relation to the collection, use and disclosure, access and correction of personal information. The key provision in relation to interference with privacy by a private sector organisation is set out in the Privacy Act s 13A (1) which provides that there is an interference with privacy in relation to personal information if the act or practice breaches a National Privacy Principle or the act or practice breaches an approved privacy code that binds the ‘organisation’.\(^{10}\)

The related NPPs which give effect and detail to the Privacy Act set the minimum standards for the collection and handling, use and disclosure of personal information about individuals, and the sharing of such information with third parties, data security, transfer of personal information, and the transborder flows of personal information.

Before examining the Privacy Act and the related NPPs, reference will be made to some key limitations on the application of the Act. The first is that the Privacy Act and the NPPs do not necessarily apply to all actors who may handle or deal with an e-commerce user’s personal information. The provisions may not apply to parties who make decisions concerning the use, application and disclosure of personal information. The second is that the Privacy Act and NPPs apply only to organisations (data collectors) as defined. Of particular importance to e-commerce users is the exemption in favour of small businesses. Thirdly, the provisions only apply to personal information contained in records.

\(^7\) The FIPs for the public sector are known as the Information Privacy Principles (IPPs).
\(^8\) Privacy Act 1988 (Cth) s14 contains the 11 IPPs, s15 relate to the application of IPPs, s16 relate to the agencies required to comply with IPPs, and sch 3 contains the 10 NPPs.
\(^9\) Refer to chapter 5 [5.2.1] on the principles and guidelines. The Privacy Act 1988 (Cth) has partially adopted the OECD principles in its IPPs and NPPs.
\(^{10}\) Additionally the Privacy Act s 13A (2) provides that the general rule will also apply to an ‘organisation that is also a credit reporting agency, a credit provider or a (tax) file number recipient.’ The Privacy Act 1988 (Cth) ss 13B, 13C, 13D contain exceptions to this rule; see also discussion in chapter 7 in relation to approved privacy codes at [7.2]-[7.3].
6.2.1 Key Limitations on the Application of the Privacy Act

6.2.1.1 ‘Organisations’

In relation to the private sector, the Privacy Act and the NPPs apply only to organisations as defined in s 6C of the Act. The Privacy Act and the NPPs (see below at [6.2.3]), impose obligations only on certain non-exempt private sector ‘organisations’ involved in the collection of ‘personal information’, and ‘sensitive information’ about an individual. The Privacy Act exempts small businesses, media, politicians and political parties, companies that are related to each other, and specified government agencies from obligations imposed on data collectors under the Act. In relation to e-commerce users, the most important exemption affecting e-commerce is the exemption of ‘small businesses’. This particular exemption will be discussed further below at [6.2.1.2].

The obligations imposed by the Act and NPPs apply only to those defined organisations involved in the collection of personal data. In contrast to the Privacy Act, the OECD Guidelines and Directive 95/46/EC use the term ‘data controller’ to describe all those who make decisions about personal data. The OECD guidelines, guideline 1(a) applies to data controllers meaning:

… a party who, according to domestic law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf.

Similarly Directive 95/46/EC art 2(d) applies to controllers, who are defined as:

---

11 Privacy Act 1988 (Cth) s 6C of the Act defines a private sector ‘organisation’ as, ‘a) an individual; or b) a body corporate; or c) a partnership; or d) any other unincorporated association; or e) a trust that is not a small business operator, a registered political party, an agency, a State or Territory authority or a prescribed instrumentality of a State or Territory’.

12 Privacy Act 1988 (Cth) s 7B exempts acts and exempt practices of organisations that include individuals (see s 7B (1)); small businesses (see s 6C); employee records (see s 7B(3); journalism (see s 7B(4)); political acts and practices (see s 7C); companies that are related to each other (see s 13B which provides for related bodies corporate and s 13B(1A) provides that the collection of personal information (other than sensitive information) about an individual by the body corporate from a related body corporate is not an interference with the privacy of an individual), and specified government agencies (see ss 7, 8); and organisations acting under Commonwealth contract (see s 7B(2)).

13 There is also an exemption in favour of related companies. This is discussed below in relation to use and third party disclosure at [6.2.2.2].

14 Refer to chapter 5 at [5.2.1.1], [5.3.2.1]; See also EC Directive 95/46/EC art 2 definition of ‘controller’ in Appendix 2.
the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data.

These broader definitions extend to those who make decisions about personal data not just those who collect, store or process that data. It is the data controller that must notify the supervisory authority of the collection, processing, purpose of collection, and expected disclosure and usage of the personal data (see chapter 5 at [5.2.1.1], [5.3.2.3]. Similarly, it is the data controller that must give notice to the data subject concerning the collection and use of that data and any security breach (see chapter 5 at [5.3.2.5]). The Privacy Act should adopt the broader terminology of data collectors to cover those making decisions about the data even if the organisation does not collect or process the data. This might be a better approach as it directly imposes responsibility on those that make decisions about the data and makes them accountable for privacy breaches.

6.2.1.2 ‘Small Business’ Exemption

Small businesses are frequently involved in e-commerce transactions and are collectors and users of personal information. It is possible that an e-commerce trader is a small business for some purposes but not for others. The Privacy Act s 6D defines a ‘small business’ as:

[A] business is a small business at a time (the test time) in a financial year (the current year) if its annual turnover for the previous financial year is $3,000,000 or less.  

15

The definition of ‘small business’ under the Privacy Act is not the same as the definition of ‘small business’ under the Corporations Act 2001 (Cth). The Corporations Act 2001 (Cth)

15 Privacy Act 1988 (Cth) s 6D(3), further identifies a ‘small business’ operator as, ‘an individual, body corporate, partnership, unincorporated association or trust that carries on one or more small businesses and does not carry on a business that is not a ‘small business’. Privacy Act 1988 (Cth) s 6DA(1), provides that the annual turnover of a business for the financial year is the total of the: ‘(a) the proceeds of sales of goods and/or services; (b) commission income; (c) repair and service income; (d) rent, leasing and hiring income; (e) government bounties and subsidies; (f) interest, royalties and subsised; (f) interest, royalties and dividends; (g) other operating income’ that is earned in the year in the course of the business. Privacy Act 1988 (Cth) s 6E, provides that a ‘small business’ operator that is a reporting entity within the meaning of the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) because of anything done in the course of a small business carried on by the small business operator are to be treated as an organisation that is required to comply with the NPPs of the Privacy Act 1988 (Cth).
defines a ‘small proprietary company’ as one having less than 50 employees. The number of private sector small businesses in Australia during the years 2000-01 was estimated to be approximately 97% of all private sector businesses. The differing definitions are confusing for small businesses when they are classified as a small business for one purpose but not for another. It maybe, however, that the emphasis on turnover in relation to e-commerce providers is appropriate to exclude small internet businesses run out of a home office or garage. So that the definition under the Corporations law is not necessarily appropriate in this context.

One of the principal reasons for the small business exemption is that many small businesses do not have significant holdings of personal information but only customer information that is used for their own business purposes and as such small businesses do not pose a high risk to privacy interests of their customers. Secondly, there is the need to balance privacy protection against unnecessary costs for small businesses. Research conducted by the Regulation Taskforce suggests that compliance for businesses can consume up to 25% of working time of large companies. The differential impact of cost of compliance for small businesses may be far greater. The Office of Small Business (OSB) estimates that the removal of the small business exemption would affect 1,805,000 businesses and the estimated total compliance cost would be $3.186 billion. The OSB also estimated that each small business would incur a start-up cost of $842 and there is an on-

---

16 Corporations Act 2001 (Cth) s 45A(2) provides that, ‘[A] proprietary company is a small proprietary company for a financial year if it satisfies at least 2 of the following paragraphs: (a) the consolidated revenue for the financial year of the company and the entities it controls (if any) is less than $25 million, or any other amount prescribed by the regulation of the purposes of this paragraph; (b) the value of the consolidated gross assets at the end of the financial year of the company and the entities it controls (if any) is less than $12.5 million, or any other amount prescribed by the regulation for the purposes of this paragraph; (c) the company and the entities it controls (if any) have fewer than 50, or any other number prescribed by the regulation for the purposes of this paragraph, employees at the end of the financial year’.


18 Privacy Act 1988 (Cth) s 6D defines a ‘small business’ as a business with an annual turnover of more than $3 million or is a health service provider.


21 Ibid.
going cost of $924 per year. The crucial question is whether the privacy of e-commerce users should be traded off against that cost.\textsuperscript{22}

Section 6EA provides that small business operators can elect to comply with the Privacy Act and NPPs. There might be some perceived benefits for small businesses to opt-in such as building brand and trust but the reality is that very small numbers opt in. Between December 2001 and end of 2006, there were only 158 small businesses that had opted-in under Privacy Act s 6EA.\textsuperscript{23} It is not known whether those that opt in may have been uncertain whether they would breach the $3,000,000 upper limit before compliance is required. This suggests that small businesses do not regard it as a priority.

The exclusion of small businesses that are private sector organisations under the Privacy Act has the effect that a very large number of small e-commerce providers are not caught by the legislation because of the annual turnover that is not more than 3 million.\textsuperscript{24} The Australian Bureau of Statistics, reported that in June 2007 there were 1,890, 213 businesses with an annual turnover of $2 million or less and this number represents 94\% of all actively trading businesses in Australia.\textsuperscript{25} The small businesses that are exempted are likely to exceed 1.9 million.\textsuperscript{26}

It is argued that privacy should not be a matter of size and that privacy as a human right should not be traded off for the benefit of commercial interests (see chapter 3 at [3.2]). An individual is entitled to have his or her private information protected even if this is a cost to businesses that collect this information. The Privacy Act should extend to all data controllers similar to that under EC Directive 95/46/EC, art 6 that requires all data controllers comply with the privacy obligations unless within the exceptions related to national security, defence, public security, and criminal law. It should also be noted that the exemption of small business is a key reason for the failure of Australian privacy

\textsuperscript{22} The OSB estimated that small businesses would have to complete the required tasks in order to comply with the Privacy Act 1988 (Cth). These tasks include: understanding and familiarising themselves with privacy legislation; conducting of a privacy audit; developing of a privacy plan; amending existing business documentation; training staff; purchasing storage of files containing personal information in a secure storage place; handling of customer complaints; record keeping; promulgation of Privacy Policy; and to update or review of a Privacy Policy. See Office of Small Business, ‘Costing into the Review of the Privacy Act 1988’, (2007) 1; Australian Law Reform Commission, above n 2, [39.167]–[39.174].

\textsuperscript{23} See Australian Government, above n 19.

\textsuperscript{24} Australian Law Reform Commission, above n 2, [39.3]–[39.33]

\textsuperscript{25} Australian Bureau of Statistics, Counts of Australian Businesses, 8165.0 (2007) 20. There were 2 011 770 actively trading businesses as at June 2007.

\textsuperscript{26} Australian Law Reform Commission, above n 2, [39.28].
legislation to meet the adequate standards test under the EU provisions (see chapter 5 at [5.3.2.1]).

While the Privacy Act exempts small businesses, the exemption does not extend to small businesses subject to the Telecommunications Act. However, this affects only a small group of providers in the telecommunications industry. The Telecommunications Act applies to ‘any person’. That would include individuals, telecommunications companies such as, carriers, ISPs, partnerships, members of the industry etc., involved with the handling of personal information through services provided by the telecommunication companies and networks.\(^{27}\) It imposes a strict regime on both large players, such as Yahoo, Google, Vodafone, etc., as well as small providers involved in the telecommunications industry. Under the Telecommunications Act pt 13, carriage service providers (CSPs) and ISPs are obliged to comply with the Act in relation to the handling of ‘affairs or personal particulars (including any unlisted telephone number or any address) of another person’.\(^{28}\) Where the regulator requires, telecommunications companies (this covers ISPs and communication network carriers) must comply with a particular industry code with no exemption for small businesses.\(^{29}\) Under Telecommunications Act pt 13, ‘eligible persons’, ‘number-database operations’ and ‘eligible number-database persons’ have an obligation to protect information or documents, that relate to an individual from disclosure unless the exceptions apply.\(^{30}\) The exceptions are referred to below at [6.2.2.2.1]). The effect is that in relation to the telecommunications sector, privacy interests have not been traded off against the compliance costs for small business. It is simply a cost of undertaking that business. A similar outcome should apply under the Privacy Act.

\(^{27}\) Telecommunications Act 1997 (Cth) s 270.

\(^{28}\) Telecommunications Act 1997 (Cth) ss 276-278; See also Australian Law Reform Commission, above n 2, [71.14] - [71.31].

\(^{29}\) Telecommunications Act 1997 (Cth) pt 13. There are currently about 1214 telecommunications companies that are listed council members of the telecommunications industry and registered with the Telecommunications Industry Ombudsman. For further details and statistics on telecommunications companies listed and registered with the Telecommunications Industry Ombudsman refer to the extract from the Telecommunications Industry Ombudsman 2010-2011 Annual Report titled A year of change available from the Telecommunications Industry Ombudsman Web site (Date accessed 2 March 2012) <http://www.tio.com.au/members/members-listing?result_8665_result_page=A>.

\(^{30}\) Telecommunications Act 1997 (Cth) s 271 defines an ‘eligible person’ as a person who is a carrier, a carriage service provider, and employee of a carrier, an employee of a carriage service provider, a telecommunications contractor, or an employee of a telecommunications contractor”; s 272 defines number-database operator” and “eligible number-database person”.

99
6.2.1.3 Personal Information

The Privacy Act only protects ‘personal information’ about an individual, if it is contained in a ‘record’ and the individual can be identified or reasonably be identified.\(^{31}\) Personal information is defined as follows in s 6(1) as:

…information or an opinion (including information or an opinion forming part of a data base), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

As noted, the section limits the application of the Privacy provisions in several ways. First, the Privacy Act s 6(1) excludes statutory protection for certain categories of personal data even if the data can identify or be linked to an individual.\(^{32}\) It excludes information in a ‘generally available publication’ which is defined in s 6 as meaning: ‘a magazine, book, newspaper or other publication (however published) that is or will be generally available to members of the public’. This would include phone books with names and addresses and such other materials as trade directories etc. A matter of special importance to e-commerce users is whether their email, or IP addresses, or web server logs are excluded. These are the means by which spam advertising, profiling and data mining occurs, (see chapter 2 [2.2.3], [2.3]). An email, IP address or a web server log would not normally be described as a ‘generally available publication’ and so would not be excluded from the operation of the Act and the NPPs as a consequence of Privacy Act s 6(1).

Secondly, the section only protects personal information contained in a record. A ‘record’ is defined in s 6 as ‘a document; or a database (however kept); or a photograph; or other pictorial representation of a person’. The definition standing on its own suggests that email

---

\(^{31}\) See Privacy Act 1988 (Cth) NPPs 7, 8; Refer also to NPP1, NPP10 in Appendix 3. Special provisions apply to ‘sensitive information’. The Privacy Act 1988 (Cth) s 6 defines ‘sensitive information’ as: ‘any information regarding race, gender, political opinion, religious beliefs, philosophical beliefs, membership of a trade union or professional organisation, or sexual preference or practices’;

\(^{32}\) Privacy Act 1988 (Cth) s 6 (1) excludes from protection records which are contained in: ‘(d) a generally available publication; or (e) anything kept in a library, art gallery or museum for the purposes of reference, study or exhibition; or (f) Commonwealth records as defined by subsection 3(1) of the Archives Act 1983 that are in the open access period for the purposes of that Act; or (fa) records (as defined in the Archives Act 1983) in the care (as defined in that Act) of the National Archives of Australia in relation to which the Archives has entered into arrangements with a person other than a Commonwealth institution (as defined in that Act) providing for the extent to which the Archives or other persons are to have access to the records; or (g) documents placed by or on behalf of a person (other than an agency) in the memorial collection within the meaning of the Australian War Memorial Act 1980; or (h) letters or other articles in the course of transmission by post’. 
and IP addresses would be excluded. But the definition must be read in conjunction with
the Acts Interpretation Act 1901 (Cth) s 2B which defines a document to include ‘any
record of information’ including ‘(c) any article or material from which sounds, images or
writings are capable of being reproduced with or without the aid of any other article or
device.’

The section defines a ‘record’ to include ‘information stored or recorded by means of a
computer’; and ‘writing includes any mode of representing or reproducing words, figures,
drawings or symbols in a visible form’ and would include emails, web server logs, or IP
addresses could qualify as a document under this definition.

A third limitation is that the protection offered applies only to personal information as
defined above, meaning that information which allows a person to make contact with
another may not qualify as personal information under the Privacy Act. Consequently,
the Act allows intrusions on the privacy of e-commerce users by allowing the harvesting of
email addresses, web server log, and IP addresses (see chapter 2 at [2.2.3]).

The fourth limitation is that under s 6 the information will only be protected if the identity
of the e-commerce user is apparent or can reasonably be ascertained. The third and fourth
limitations raise important questions as to what information may be relied on to identify
the user, and what information is protected.

The definition of ‘personal information’ under the Privacy Act s 6 does not state that the
individual’s identity must be able to be ascertained only from the information collected. If
it did, then it would only apply to the information recorded against an identification
number, IP addresses and passwords. One reason why the Privacy Act does not explicitly
deal with email addresses, IP addresses and weblogs is that the Privacy Act provisions are
based on the OECD Guidelines which were developed in the 1980’s when information
technology was in its infancy and information that could identify a person such as IP

---

33 Nor is it protected under the Telecommunications Act 1997 (Cth); See Australian Law Reform
Commission, above n 2, [71.110].
34 Privacy Act 1988 (Cth) NPP8 provides that ‘whenever it is lawful and practicable, individuals must have
the option of not identifying themselves when entering transactions with an organisation’.
35 Privacy Act 1988 (Cth) NPP7 defines an identifier as including ‘a number assigned by an organisation to
an individual to identify uniquely the individual for the purposes of the organisation’s operations’. NPP7
only regulates the handling by organisations of identifiers assigned by agencies such as tax file number. An
individual’s name and Australian Business Number (ABN) are explicitly excluded from being considered
identifiers for the purposes of the NPPs.
addresses, email address, or passwords were non-existent. So there is no mention in the OECD Guidelines, or in the Privacy Act whether email, IP addresses and web server logs are included or excluded as personal information. The issue could be put beyond doubt by defining personal information to include email, IP addresses and web server logs.\(^\text{36}\) Currently, it is left to the general provision under Privacy Act s 6, that the information is personal only if the identity of the person is apparent or reasonably ascertainable.

Whilst it is clear that IP addresses and domain information such as ‘uws.edu.au’ allows the geographical and system location of the computer to be identified, it can also identify the person delegated with the responsibility to allocate the machine’s address.\(^\text{37}\) Moreover email addresses if sufficiently related to the individual can also lead to identification. These identifiers may allow individuals to be identified, contacted, or tracked for example by using an e-commerce user’s email address, or an internet protocol (IP) address.\(^\text{38}\) But as mentioned earlier, these addresses may not qualify as personal information protected by the Privacy Act if all they do is allow contact with the individual.

The further difficulty is determining what will be regarded as ‘reasonably’ ascertainable. The Australian Law Reform Commission proposed that the test of whether a person is reasonably ascertainable is whether the individual can be identified from information in the possession of an organisation or from that information and other information the organisation may access ‘without unreasonable cost or difficulty’.\(^\text{39}\) It should be noted that the suggested test refers to whether the organisation can identify the individual. The problem is that if an organisation discloses non-identifying information, outsiders may, with some effort, ascertain the identity of an individual. Web users unintentionally reveal personal information about themselves when they use search engines. It is risky when companies such as AOL, Google and Yahoo compile detailed records of web searches conducted by individuals and circulate it online. Such was the case with the release of search queries by web surfers that are collected and released by AOL.\(^\text{40}\) If the prime


\(^{38}\) Refer to [6.2.1.3] above to the discussion on the type of information protected under the Privacy Act 1988 (Cth).

\(^{39}\) See Australian Law Reform Commission, above n 2, [6.55]–[6.60]. The ALRC also recommended that guidelines for determining should be developed by the Information Commissioner.

\(^{40}\) Michael Barbaro and Tom Zeller Jr, above n 36.
purpose is to protect the individual e-commerce user’s privacy, then it is suggested that a broader test should be applied rather than one limited to whether the organisation can ascertain identity. The test should be whether the general public could reasonably ascertain the identity of the person concerned if the information were to be disclosed.

If email, IP addresses do not qualify as ‘personal information’, it allows the collection of personal information such as consumption habits of e-commerce users using the Internet for e-commerce transactions or using Internet search engines.\footnote{See discussion in chapter 5 [5.2.1.2], [5.3.2.2] on how IP addresses are being used to identify individuals. See also detailed opinion of the Working Party 29 Data Protection Commissioner about search engines in Article 29 Data Protection Working party, Opinion 1/2008 on data protection issues related to search engines, WP148, adopted 4 April 2008; see also EFA Submission to the Inquiry into the Privacy Act 1988 conducted by the Senate Legal & Constitutional References Committee, (24 February 2005) <http://www.efa.org.au/Publish/efasubm-slrc-privact2005-suppl.html.}

An individual’s unique interests and consumption habits may be such that they could be linked to the individual.\footnote{See OECD Guidelines, Explanatory Memorandum: Automated and non-automated data [35]; See also Directive 95/46/EC Recitals [27], art 2 in Appendix 2. As was previously noted in chapter 5 [5.3.2.1], [5.3.2.3], Directive 95/46/EC art 2(4) defines processing of personal data to include the process of collection, use and/or disclosure, sharing, and transfer of personal information. It captures not only manual collection but also includes automatic processing of personal data. It clearly covers data mining and similar processes which may not be covered by the Privacy Act because of its limitation to personal information contained in records.}

Protection could be given to this type of information by extending the definition of ‘personal information’ under the Privacy Act to cover identifiers (including IP and email addresses) irrespective of whether it is obvious to the collector or discloser that an individual’s identity can reasonably be ascertained from that identifier and/or whether or not an individual can be contacted by use of the identifier.\footnote{Refer to Privacy Act 1988 (Cth) sch 3 NPP7 in Appendix 3.}

The Privacy Act could be amended so that the definition of ‘personal information’ and the requirement that it be contained in a record specifically includes email addresses and passwords, transaction details, Internet user’s machine ID, IP addresses, User ID, and web server logs all of which can be used to identify the individual.

In contrast to the definition of personal information under the Privacy Act s 6, the EC’s Directive 95/46/EC art 2 defines ‘personal data’ as ‘any information relating to an identified or identifiable natural person (‘data subject’); and an identifiable person as ‘one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, psychological, mental, economic, cultural or social identity’ (see chapter 5 at [5.3.2.2]).\footnote{Michael Barbaro and Tom Zeller Jr, above n 36.} This broader definition captures a
wider variety of information than under the Australian definition. It extends to the indirect identification and is not qualified by the requirement that the person be ‘reasonably identifiable’. The broader definition can cover information in any form, digital and manual, that can directly or indirectly link and/or identify individuals and would cover identifiers that include emails, IP addresses, passwords and web server logs. The provision under Directive 95/46/EC is broader, sufficiently flexible and technology neutral to allow for new ways that information can identify an individual and should be adopted in Australia. All types of personal data, unless such data is rendered anonymous in such a way that the data subject is no longer identifiable should be protected equally under the Privacy Act. The EU provision provides an appropriate model for adoption. Considered next are the Privacy Act NPPs.

### 6.2.2 The National Privacy Principles (NPPs)

There are ten NPPs and compliance with them by the non-exempt private sector data collectors is mandatory unless they are bound by an equivalent industry code (see chapter 7 at [7.2]). The ten NPPs are substantially based on the OECD Guidelines. They are interrelated and overlap in their application, and so must be taken as a whole. Their intent is to improve and maintain better information handling standards. The NPPs are: NPP1 – Collection; NPP2 – Use and disclosure; NPP3 – Data Quality; NPP4 – Data Security; NPP5 – Openness; NPP6 – Access and correction; NPP7 – Identifiers; NPP8 – Anonymity; NPP9 – Transborder Data Flows; and NPP10 – Sensitive Information.

Each of the above is discussed below in relation to: Collection (NPPs 1, 10, 5); Use and disclosure, and the sharing of personal information collected with third parties (NPP2); Access and correction (NPPs 3, 5, 6); Data security (NPP4) and International flows of personal information (NPP9).

#### 6.2.2.1 Collection (NPPs 1, 10, 5)

The Privacy Act NPP1 provides for the collection of ‘personal information’ and NPP10 relates to the collection of ‘sensitive information’. NPP1 provides that personal

---

45 See extract of the NPPs in Appendix 3.
46 Privacy Act 1988 (Cth) s 6 defines sensitive information as, ‘information regarding race, gender, political opinion, religious beliefs, philosophical beliefs, membership of a trade union or professional organisation, or sexual preference or practices’.
information can only be collected about individuals if the collection of such information is lawful and relevant for the legitimate purposes of the organisation, and to the extent necessary for those purposes and collected by fair means (NPP1). An organisation must not collect personal information in ‘an unreasonably intrusive way’ (NPP1.2). Under NPP1, if it is reasonable and practicable to do so, personal information about an individual must be collected only from that individual (NPP1.4). If a data collector collects personal information about an individual from a third party, then NPP1.5 provides that the data collector must take reasonable steps to ensure that the individual is, and/or has been made aware of the matters listed in NPP 1.3 unless the exceptions apply. NPP1.3 in particular provides that:

...an organisation must at the time (or, if not practicable, as soon as practicable after) that an organisation collects personal information about an individual from the individual itself, then that organisation must take reasonable steps to ensure that the individual is aware of:
(a) the identity of the organisation and how to contact it; and
(b) the fact that he or she is able to gain access to the information; and
(c) the purposes for which the information is collected; and
(d) the organisations (or the types of organisations) to which the organisation usually discloses information of that kind; and
(e) any law that requires the particular information to be collected; and
(f) the main consequences (if any) for the individual if all or part of the information is not provided.

There are also special provisions relating to the collection of ‘sensitive information’ (NPP 10) which requires prior consent of the data subject. Under NPP10 a more direct link to

---

47 See Privacy Act 1988 (Cth) sch 3 NPP 1 in Appendix 3; Refer also to the 1980 OECD Guidelines, Collection Limitation Principle in chapter 5 [5.2.1.2]; See also discussion on EC Directive 95/46/EC arts 10, 11 in chapter 5 [5.3.2.3]. Article 10 that provides for information to be given to the data subject in cases of collection of data from data subject and art 11 provides for information to be given to the data subject in cases where data is not collected from data subject.

48 Privacy Act 1988 (Cth) sch 3 NPP1.1–1.3 in Appendix 3. NPP1.3 provides a list of information that the data collector is required to give to the data subject. This includes the identity of the data collector; how to contact the data collector to ascertain how it had gained access to that information; the purposes for which the information was collected; and to whom the organisations disclose such information.

49 See Privacy Act 1988 (Cth) NPP1 in Appendix 3.
the primary purpose of collection is required in relation to ‘sensitive’ information’. NPP10.2 and NPP10.3 provide some exceptions, in particular where ‘sensitive information’ about individuals can be collected without consent. A data collector is exempt from taking reasonable steps to ensure that an individual is aware of the data collected if making the data subject aware would be a serious threat to the life and health of any individual. The exceptions for the requirement for consent are: firstly, the information must relate solely to the members of the organisation or to individuals who have regular contact with it in connection with its activities; secondly at or before the time of collecting the information, the organisation undertakes to the individual that the organisation will not disclose the information without the individual's consent; or thirdly if the collection is necessary for the establishment, exercise or defence of a legal or equitable claim.

One of the key problems in relation to NPP1 is that there is no separate or express provision dealing with collection of personal information from third parties under the NPPs. NPP1.5 provides that it is sufficient if the organisation collecting the information from a third party takes reasonable steps to ensure that the data subject is made aware of the matters listed in NPP1.3, unless making the data subject aware of the information collection would pose a threat to the life or health of any individual. It does not directly impose an obligation on the third party who may or may not be subject to the Privacy Act and the NPPs. In the absence of monitoring, it is not clear whether organisations actually comply with these requirements. This contrasts with the EC Directive art 10 which provide that if the data has not been obtained from the data subject then the data controller or his representative have the following obligations. They must at the time of recording the data (or if a disclosure to a third party is envisaged) provide information to the data subject as to: the identity of the controller or of his representative; the purpose of processing (collection, use and disclosure) (see art 11); information about the categories of data collected; the recipients of such data, and the right to access and rectify (see art 12). It imposes an absolute obligation rather than a qualified duty to take reasonable steps as is

---

50 Currently NPP10 covers the collection of ‘sensitive information’. The ALRC has recommended that the collection of sensitive information by organisations should be contained in the ‘Collection Principle. See Australian Law Reform Commission, above n 2, [21.60]–[21.61], [22].

51 See NPP10.1 in Appendix 3. NPP 10.1 provides that an organisation must not collect sensitive information about an individual unless (a) the individual has consented, (b) the collection is required by law; or (c) the collection is necessary to prevent or lessen a serious and imminent threat to the life of health of any individual.

52 Privacy Act 1988 (Cth) sch 3 NPP 10.1(a).
the case under NPP1.3. This approach gives preference to the privacy rights of the e-commerce user over the commercial costs for the e-commerce provider.

NPP1.3 does not impose obligations to post privacy policies on websites. Nor is there a requirement that all e-commerce users have easy access to those policies. The organisation need only take reasonable steps to ensure that the individual is aware of certain matters at the time of collection or as soon as practicable thereafter:

- the identity of the organisation, its contact details,
- how the individual can gain access to the information collected,
- the purpose for which the information is collected,
- the type of organisations to which the organisation usually discloses information of that kind, if the collection of such personal information is required by law, and
- the main consequences (if any) for the individual if all or part of the information is not provided.

It is surmised that most e-commerce providers rely on acknowledgement on the website by the e-commerce user of the contents of its privacy policies to provide the required information. NPP5 provides for transparency in information collection. NPP5.1 requires that the organisation set out in a document clearly expressed policies on its management of personal information and make it available to anyone who asks for it. This makes it very unlikely that an e-commerce user wanting to purchase goods or services would go to the effort of formally requesting the policy document. Under NPP5.2 on request by a person, an organisation must take reasonable steps to let the person know, generally, what sort of personal information it holds, for what purposes, and how it collects, holds, uses and discloses that information. As it puts the onus on the e-commerce user to request the document, it serves to preference to the interests of the organization over that of the e-commerce user. The ALRC has recommended a separate ‘Openness’ principle requiring organisations to set out clearly expressed policies on its handling of personal information.

53 But note NPP 5 discussed below.
54 NPP1.5 provides that if the information about the individual is collected from someone else then the organisation collecting such information must comply with the requirements under NPP1.3 except if making the individual aware of the matters would pose a serious threat to the life or health of any individual. See Appendix 3. NPPs 1, 2 reflect the OECD principles on collection limitation, and use limitation.
Chapter 4 examined the efficacy and problems arising from standard form privacy policy statements used by ISPs, e-businesses and Internet websites. While there may be formal compliance with the requirements of the NPPs concerning notification of collection etc., there are significant problems with privacy policies and clauses which are not necessarily overcome by the ALRC proposal set out above. Chapter 4 recommended that an organisation's privacy policy be easy to find, read and understand and available prior to or at the time that individually identifiable information is collected or requested. So the privacy policy must clearly state in simple language: what information is being collected; the use of that information; possible third party distribution of that information; the choices available to an individual regarding collection, use and distribution of the collected information; a statement of the organisation's commitment to data security; and what steps the organisation takes to ensure data quality and access.

The Collection Principle does not expressly impose an obligation to notify e-commerce users whose personal information has been, (or is to be collected) of the matters set out in NPP1.3. The ALRC recommended the adoption of a separate notification principle. In contrast to Privacy Act, NPP1, the OECD Guidelines’ Collection and Openness Principle, and Directive 95/46/EC arts 10-11 and 18 have separate provision for mandatory notification prior to data collection (see chapter 5 at [5.3.2.3]). Directive 95/46/EC art 10, provides that a data controller or his representative is required to provide information to the data subject about the source of the information, the identity of the data collector and his representative if any, information about recipients of the data, information about the existence of a right to access and rectify incorrect data, (see chapter 5 at [5.3.2.3.1(c)]). Article 11 similarly imposes responsibilities for notification to the data subject if the personal data is not directly obtained from the data subject. Directive 95/46/EC art 18

55 The ALRC recommends that the document should include: what sort of personal information the agency or organisation holds; the purpose for which personal information is held; the steps individuals may take to access and correct personal information about them held by the agency or organisation; and the avenues of complaint available to individuals in the event that they have a privacy complaint.’ Refer to ALRC, above n 2, [24.61] 822.

56 This would oblige the e-commerce provider to take ‘such steps, if any, as are reasonable in the circumstances’ to notify or otherwise ensure that an individual is aware of ‘specific matters’. Refer to ALRC, above n 2, [23.16].

57 Directive 95/46/EC art 11 provides that if information about the data subject is not collected from the data subject then the controller or his representative must at the time of undertaking the recording of personal data
provides that a data controller or his representative must notify the supervisory authority referred to in art 28 before carrying out any wholly or partly automatic processing operation or set of such operation intended to serve a single purpose or several related purposes (see chapter 5 at [5.3.2.1 (a)]). In addition, EC Directive 95/46/EC art 19 provides for the content of the notification. This is not currently required under the Australian Privacy Act or NPPs.

The Privacy Act should require prior notification of the collection of personal information to the supervisory authority as well as to the individual e-commerce user. This will enable greater transparency of who is collecting information, for what purposes and the use and recipients of this information. It will allow appropriate correction and notification as well as more effective monitoring of compliance (see discussion in chapter 8 at [8.3]). If there is effective communication to e-commerce users at the initial collection of personal information, this will allow e-commerce users to make choices in relation to their personal information. Optimally, two separate provisions would be required: firstly notice prior to collection to the supervisory authority, the Australian Information Commissioner; and secondly notice to the e-commerce user prior to personal information or sensitive information collection. This will give the e-commerce user greater control over their personal and sensitive information similar to EU citizens.

6.2.2.1.1 Consent and Collection of Personal Information

An e-commerce provider may require an e-commerce user to expressly consent to the collection of personal information. Chapter 4 examined the role of consent in the waiver of privacy rights. It pointed to the significant problems with mechanisms for obtaining consent by e-commerce users. This section examines the requirements prior to collection of personal information under the NPPs.

or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed provide the data subject with at least the following information, except where he already knows the information as required under art 10. The 2012 reform proposals, in addition to the above requirements, the data subject must also be informed about the right to lodge a complaint and the contact details of the supervisory authority (see art 14(1) (e)), as well as whether it is intended to transfer data to a third country and the level of protection available in that third country (see art 14(1) (g)). See European Commission, Proposals for a Regulation of the European parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) Brussels, 25 January 2012 COM(2012) 11 final 2012/0011 (COD).
NPP 1.3 requires only that the individual is aware of collection at or before the time of collection where practicable. It does not require consent to collection. With respect to sensitive personal information, NPP10 provides that prior consent must be obtained. Despite this, the reality is that consent is frequently perfunctory (see chapter 4 at [4.2]). The Australian position contrasts with the Directive 95/46/EC under which data collectors must obtain an individual’s ‘explicit and unambiguous consent’ prior to processing of personal information (see Directive 95/46/EC arts 2 (h), 7(a)). The OECD Guidelines require actual knowledge and consent prior to collection. The higher standards imposed by the EU and OECD give greater recognition to privacy as a human right. Australian e-commerce users consequently have less protection than EU citizens. Equivalent protection would require that data collectors register before collecting information and that information can only be collected where there is prior consent by the e-commerce user.

6.2.2.2 Use and Third Party Disclosure (NPP2)

NPP2 deals with use and disclosure of personal information. It provides that:

…an organisation must not use or disclose personal information about an individual for a purpose (the secondary purpose) other than the primary purpose of collection unless:

(a) both of the following apply:

(i) the secondary purpose is related to the primary purpose of collection and, if the personal information is sensitive information, directly related to the primary purpose of collection;

(ii) the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose; or

(b) the individual has consented to the use or disclosure;

(c) if the information is not sensitive information and the use of the information is for the secondary purpose of direct marketing:

58 See Appendix 2 for the definition of ‘processing of personal data’ under Directive 95/46/EC art 2.
59 NPP1.5 provides that if the information about the individual is collected from someone else then the organisation collecting such information must comply with the requirements under NPP1.3 except if making the individual aware of the matters would pose a serious threat to the life or health of any individual. See Appendix 3. NPPs1, 2 reflect the OECD principles on collection limitation, and use limitation discussed in chapter 5 [2.1.1], [5.2.1.4].
(i) it is impracticable for the organisation to seek the individual's consent before that particular use; and

(ii) the organisation will not charge the individual for giving effect to a request by the individual to the organisation not to receive direct marketing communications; and

(iii) the individual has not made a request to the organisation not to receive direct marketing communications; and

(iv) in each direct marketing communication with the individual, the organisation draws to the individual's attention, or prominently displays a notice, that he or she may express a wish not to receive any further direct marketing communications; and

(v) each written direct marketing communication by the organisation with the individual (up to and including the communication that involves the use) sets out the organisation's business address and telephone number and, if the communication with the individual is made by fax, telex or other electronic means, a number or address at which the organisation can be directly contacted electronically.  

Its effect is discussed under the following headings: (1) use for related secondary purposes where the e-commerce user would reasonably expect disclosure or use for those purposes; (2) direct marketing

6.2.2.2.1 Secondary Use and/or Disclosure

Secondary disclosure and usage is permitted where the e-commerce user consents under NPP2 or where the use or disclosure to another party is for a secondary purpose, which is related to the primary purpose for which the information is collected and the ‘individual would reasonably expect the organisation to use and/or disclose the information for the secondary purpose’.  

The reasonable expectation requirement is meant to be understood in a common sense way and is not overly onerous. For example, if a person has several different types of contact with one bank, he or she could expect the information about themselves to be shared within that bank. If the banking group also ran a health insurance business, the individual

60 Privacy Act 1988 (Cth) sch 3NPP2.
61 Privacy Act 1988 (Cth) sch 3 NPP 2.1(a) (ii).
62 See Australian Law Reform Commission, above n 2, [25.39].
would not expect their health claims record to be matched with banking information. Similarly, for example, where delivery or billing is subcontracted out by the e-commerce provider, the disclosure and use of personal information for delivery and billing purposes would be regarded as sufficiently related to the primary purpose of collection. If an entity is unsure of the reasonable expectations of an individual in particular circumstances, it could seek the individual’s consent. This issue does not arise under the OECD Guidelines Purpose Specification, and use limitation principle (see chapter 5 at [5.2.1.4]) or under the EU provisions which require prior notification to the supervisory authority before collection of data with details of all proposed usage of the collected information, Directive 95/46/EC, art 18. The prior notification to the supervisory authority allows collection, processing, usage, disclosure and transfer of data to be monitored to ensure that it is only used for purposes as stipulated in the notification. The dual requirement for consent prior to collection and notification to the data subject allows the e-commerce user to make choices in relation to her or his personal information and usage and disclosure of that data. The proposed reform to Directive 95/46/EC introduces a new approach. Under the proposed articles 22(1) and (3), data controllers must now adopt policies and implement appropriate measures to ensure and to be able to demonstrate compliance with the data protection rules and to ensure that the effectiveness of the measures and these must be verifiable. The EU provisions allow monitoring and verification that privacy obligations are being satisfied (see chapter 5 at [5.3.2.3]). There are no similar provisions or proposals in relation to Australia. Moreover, in contrast to Directive 95/46/EC art 18, there is no such mandatory notification provision under the Privacy Act and it appears to give precedence to the economic interests of the e-commerce provider.

In relation to the small cohort of e-commerce providers who come within the provisions of the Telecommunications Act, there are different requirements for compliance.

---

63 Directive 95/46/EC art 19 provides that the content of notification must include: (a) the name and address of the controller and of his representatives if any; (b) the purpose or purposes of the processing; (c) a description of the category or categories of data subject and of the data or categories of data relating to them; (d) the recipients or categories of recipient to whom the data might be disclosed; and (e) the proposed transfer of data to third countries; (f) a general description allowing a preliminary assessment to be made of processing.’
65 Ibid, II.6 Controller and processor (Chapter IV), [WP 166-173].
66 See discussion in chapter 5 [5.3.2.3]; See also above n 57, art 14. In addition to the requirements under arts 18 and 19 of Directive 95/46/EC, the proposed reform under art 14(1) (a) provide that an organisation must also have a data protection officer responsible for compliance with the regulation.
67 Refer to discussion in relation to NPP1.3 above at [6.2.2.1].
Telecommunications Act pt 13 regulates the use and disclosure of personal information related to contents or substance of communications carried, or being carried, by a carrier or carriage service provider. In relation to telecommunications service providers, personal information of a third party may also be included such as in a bill for calls made to a telephone number and location of the third party that can also identify the third party individual. The Telecommunications Act ss 279 and 296 allow the use and disclosure of personal information if the use or disclosure is made ‘in the performance of the person’s duties as an employee or contractor’.

More importantly for the purposes of e-commerce users, Telecommunications Act s289 allows use and disclosure when the individual is "reasonably likely to have been aware or made aware" that the information is usually disclosed or used for the secondary purpose/s. Consequently organisations involved in the telecommunications industry can merely notify individuals they intend to use and disclose personal information (including sensitive information) for secondary purposes. This amounts to significant inroads to the personal privacy of e-commerce users. It is not limited to usage that is necessary for the primary purposes. Nor does it require an e-commerce user’s consent to this secondary use. Secondary use or disclosure should be permitted only with the individual’s consent; and if such information is used or disclosed for secondary purposes it is only used or disclosed if it is necessary to provide a particular service or where a public interest exceptions apply.

Additionally, the Telecommunications Act s 290 recognises implicit consent of sender and recipient of communications to disclosure of content of communications if ‘it might reasonably be expected that the sender and the recipient of the communication would have consented to the disclosure or use, if they had been aware of the disclosure or use’.

---

68 Telecommunications Act 1997 (Cth) pt 13 protects ‘personal particulars. Section 276 provides that ‘personal particulars’ include ‘any unlisted telephone numbers or any address’. In relation to Internet based applications, the information protected under pt 13 include IP address used for the session and the start and finish of each session.

69 Telecommunications Act 1997 (Cth) ss 276-278. See Australian Law Reform Commission, above n 2, [71.17].

70 See discussion in relation to web server log information and location based information below at [6.3.1].


72 It provides that, ‘Section 276 does not prohibit a disclosure or use by a person if: (a) the information or document relates to the contents or substance of a communication made by another person; and (b) having regard to all the relevant circumstances, it might reasonably be expected that the sender and the recipient of the communication would have consented to the disclosure or use, if they had been aware of the disclosure or use’.
Section 290 is obviously essential to permit normal communications. So the sender of information to be displayed on a website could be assumed to have consented to the recipient displaying the material on the website. Although s 290 adopts the similar language of ‘reasonable expectation’ as the Privacy Act provision, there may be subtle differences. Under the Telecommunications Act s 290, the ‘reasonable expectation’ relates to whether the individual would have consented to that use, whereas under the Privacy Act it is the ‘reasonable expectation’ of use or disclosure of the personal information. In either case, the objections mentioned previously apply equally: the individual should know at the outset the person who is going to use their personal information, and for what purpose. This should, as in the EU, be notified to the e-commerce user prior to collection.

6.2.2.2.2 Direct Marketing

Direct marketing represents over 50% of all media spending – it is a huge and expensive industry. A 2007 survey by the Privacy Commissioner indicated that 80% of respondents had expressed concern or annoyance about receiving unsolicited direct marketing communications. An individual receiving direct marketing may not always know what personal information about them has been collected or that their personal information has been collected for the purpose of direct marketing. The promotion and sale of goods and services by direct marketers include unsolicited and direct marketing based on lists of personal information such as names and contact details compiled from a various sources. There is a possibility that personal information has been collected without consent and compiled into a list that may be used or sold to another organisation for the purpose of direct marketing.

The Privacy Act NPP 2.1(c) allows secondary use for direct marketing purposes without express consent. NPP2.1(c) only requires that all organisations sending direct marketing communications to individuals advise them of their right to opt-out and provide information on how to do so. So under Privacy Act NPP2.1(c) (iv), the collector is only required to draw to the individual’s attention, or prominently display a notice, that he or

76 Privacy Act 1988 (Cth) sch 3 NPP2.1(c) (iii)-(iv).
she may express a wish not to receive any further direct marketing communications. Under NPP2.1(c) (v), the written direct marketing communication by the organisation with the individual should set out the organisation’s business contact details so that the organisation can be directly contacted electronically.

This contrasts with the approaches adopted by the OECD guidelines and Directive 95/46/EC. The OECD’s Use Limitation Principle requires that personal data should not be disclosed, or made available or otherwise used for purposes other than with the consent of the data subject; or by the authority of law in accordance with the Purpose Specification Principle. Under Purpose Specification Principle, the purpose specified at the time of the collection restricts the use of the information collected. A data subject can object to the processing of personal data at no cost to them and without having to state reasons. Under the Purpose Specification Principle, when the data collected has served its purpose it should be destroyed or erased or given an anonymous form.77 Directive 95/46/EC art 6 provides that personal data must be collected for a specific, explicit and legitimate purpose. Most importantly Directive 95/46/EC art 14 gives the data subject a right to object at any time on compelling legitimate grounds to the processing of data relating to him or her (see chapter 5 at [5.3.2.3]). Under reform proposals it will be up to the controller to demonstrate compelling legitimate grounds for the processing of data which overrides ‘the interest or fundamental rights and freedoms of the data subject.’78 The data subject also has the right to object to the processing of personal data for the purpose of direct marketing, and to be informed before personal data is disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses (see Directive 95/46/EC art 14(b)). There are no equivalent requirements under the NPPs although NPP5 requires an organisation to provide information to the individual (on request) on the type of personal information that is held, used and disclosed by the data collector.79 It is thus apparent that the current NPPs give preference to commercial interests in allowing direct marketing without consent. Chapter 4 has noted the problems with opt out provisions and the preference for opt in provisions (see chapter 4 [4.2.1.2]).

77 The reason for this is that control over data may be lost when data is no longer of interest. Keeping data after it has served its purpose may also lead to risk of theft, unauthorised copying.
78 See European Commission, above n 57.
79 Privacy Act 1988 (Cth) sch 3 NPP5.1-5.2.
NPP2.1 provides no effective mechanism for the individual to withdraw consent when their personal information that is collected for primary purposes and used for secondary purposes nor does it provide an opt-out mechanism except in relation to direct marketing.\(^{80}\) NPP2 does not directly address the issue of whether it applies to information obtained through data mining and electronic surveillance of e-commerce users and Internet users.\(^{81}\) In contrast, these usages are not permitted under the OECD principles without the consent of the e-commerce user and without prior specification of this usage prior to collection.\(^{82}\) In contrast to NPP2, Directive 95/46/EC art 6 requires that all data processing must be consented to by the data subject either under contract, or if there is a legal obligation to provide such personal data under art 5.\(^{83}\) So in the EU, the e-commerce user is potentially aware of all primary and secondary usage. But in relation to Australia, an e-commerce user does not necessarily know or consent to secondary usage. So it appears that Directive 95/46/EC art 6 provides greater protection to e-commerce users than the NPPs.

6.2.2.2.3 Direct Marketing – NPP 2 (c) and the Spam Act 2003 (Cth)

The Privacy Act and the Spam Act overlap in their application. As noted above NPP 2(1) (c) provides an opt-out mechanism for those who do not wish to receive direct marketing communications. An opt-out mechanism is not the preferred option for ensuring that e-commerce users actively consent to collection, disclosure or use of personal information (see chapter 4 [4.2.1]). In relation to direct marketing, the NPPs must be read in conjunction with the Spam Act 2003 (Cth). In contrast to NPP2, the Spam Act sets out three requirements to be met prior to sending an email to a recipient. These are:

- Firstly, prior consent must be obtained. Consent may be express or may be inferred based on a business or other relationship with the recipient;\(^{84}\)
- Secondly, the commercial message must always contain clear and accurate identification of who is responsible for sending the message and how they can be contacted;\(^{85}\) and

\(^{80}\) Refer to discussion on NPP2.1(c)) below at [6.2.2.2.3].
\(^{81}\) Privacy Act 1988 (Cth) sch 3 NPP2.1 (a) (i)-(ii).
\(^{82}\) OECD Guidelines Purpose Specification principle 9 provides that ‘the purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose’.
\(^{83}\) Directive 95/46/EC art 5 provides that, ‘Member States shall, within the limits of this Chapter determine more precisely the conditions under which the processing of personal data is lawful’.
\(^{84}\) Spam Act 2003 (Cth) sch 2 s 4.
Thirdly, the commercial message should contain an unsubscribe facility that allows the recipient to indicate that such messages should not be sent to them in future. \(^{86}\)

Under the Spam Act, consent to the sending of unsolicited electronic commercial emails may not be inferred unless there is an existing business or other relationship; where there is a reasonable expectation by the individual that they may receive commercial electronic messages; and in circumstances in which there is conspicuous publication of work that relates to an electronic address as in a social networking website, a subscription to a magazine, or a website. \(^{87}\) If such publication includes a statement that the person does not want to receive unsolicited commercial electronic messages at that address then the organisation cannot infer consent. \(^{88}\) This includes messages that aim to gauge the recipient’s interest in receiving future electronic commercial messages seeking to establish a commercial relationship.

The exception is where the purpose of the email is of a contractual, operational or service related customer notice. Spam Act sch 2 s 4(2), provides that consent may be inferred if the particular electronic address enables the public, or sections of the public to send electronic messages to a particular individual, employee of an organisation, a partner in a partnership, a self-employed individual within the organisation; if the electronic address has been conspicuously published, and it would be reasonable to assume that the publication occurred in agreement with the individual or organisation. Where an organisation holds an email address of a customer, or subscriber to a service such as reward points or someone that it deals with on an ongoing basis, consent to receiving electronic messages from the organisation may be inferred. In this case there may be reasonable expectation by the individual that they may receive commercial electronic messages.

The Spam Act does not cover non-electronic messages such as ordinary mail, paper flyers; voice to voice telemarketing; a majority of ‘pop up’ windows that appear on the internet; and messages without any commercial content that do not contain links or directions to a commercial website or location. \(^{89}\) The Spam Act covers commercial electronic messages

\(^{85}\) Ibid, ss 3, 17.

\(^{86}\) Ibid, ss 3, 18.

\(^{87}\) Ibid, s 4(1) provides that consent of the relevant electronic account-holder may not be inferred from the mere fact that the relevant electronic address has been published.


\(^{89}\) Spam Act 2003 (Cth) s 5(5).
such as direct marketing emails, instant messaging, SMS text messaging, text and image-based mobile phone messaging (MMS) \(^{90}\) that originate in Australia and are sent to any destination; and those originating overseas sent to an address in Australia. \(^{91}\) It defines a commercial electronic message as any electronic message that offers, advertises or promotes the supply of goods, services, land or business or investment opportunities; advertises or promotes a supplier of goods, services, land or a provider of business investment opportunities; assist a person to dishonestly obtain property, commercial advantage or other gain from another person. \(^{92}\) The Act makes it illegal to send, cause to be sent, unsolicited commercial electronic messages including instant messaging, SMS, and MMS (text and image-based mobile phone messaging). \(^{93}\)

Under the Spam Act harvested-address lists including lists (collection or compilation) of electronic addresses using address harvesting software or harvested-address lists must not be supplied, acquired or used. \(^{94}\) These prohibitions are much more extensive than under the Privacy Act, where email and IP addresses are not within the definition of ‘personal information’ or ‘sensitive information’ and are not protected (see above at [6.2.1.1], [6.2.1.2]). So the use of email addresses and IP addresses that may be harvested using data mining technology and later used for direct marketing or the use and/or disclosure of such information to third parties without the express prior consent of an individual recipient of electronic commercial messages will not be a breach under NPP2. NPP 2.1(c) (i)) permits the transfer of direct marketing messages without consent, whereas the Spam Act requires that prior consent of the recipient must be first obtained. \(^{95}\)

The Spam Act creates conditions in which it is for the sender to prove that consent exists. In contrast, under the Privacy Act the burden is shifted to the individual to prove that their personal information was collected or used and/or disclosed without their consent or in breach of the NPPs.

---

\(^{90}\) Ibid, s 3.
\(^{91}\) Ibid, ss 7, 13-14.
\(^{92}\) Ibid, s 6.
\(^{93}\) Ibid, s 15-18. Section 15 of the Act provides that unsolicited commercial electronic messages must not be sent, secondly commercial electronic messages must include information about the individual or organisation who authorized the sending of the message; and thirdly commercial electronic messages must contain a functional unsubscribe facility.
\(^{94}\) Spam Act 2003 (Cth) pt 3 ss 19-22.
\(^{95}\) Ibid, sch 2 s 4 specifies that consent can be express or can be reasonably inferred from the conduct of the business and the relationships of the individuals, or organisation concerned.
The Spam Act responds to community and business concern over the volume of unsolicited email advertising. It provides clear advantages over the existing NPPs in a number of respects: firstly, the requirement of a clearly identified unsubscribe mechanism; secondly, the prohibition of email harvesting; and thirdly, the prohibition of direct advertising without prior consent or in circumstances where consent might properly be inferred. In relation to electronic messaging, the NPPs should be amended consistent with the approach to direct marketing adopted by the Spam Act. This divergence further emphasizes the problems when privacy is regulated under multiple pieces of legislation involving different regulators with inconsistent approaches. This thesis argues that privacy matters should be dealt with under a single legislative mandate and a single regulatory authority. See further discussion below at [6.2.2.5.3].

Although under the NPPs, the individual can choose to opt-out of secondary usage for direct marketing purposes (see above), the preferred approach is that adopted in the OECD and Directive 95/46/EC by requiring up front consent to disclosure and use of personal information. Australian privacy law secondary use principles give primacy to commercial interests over the privacy interests of the e-commerce user. Privacy as a human right should not yield to political and commercial interests. This is reflected in Directive 95/46/EC art 6, which prohibits secondary use without prior consent. It is recommended that the Privacy Act adopt similar provisions as those under Directive 95/46/EC art 10, so that all data collectors provide individuals in Australia information about who has access to information about them, how that information is going to be used; and what type of information is out there about them so that they are able to make the choice as to whether to consent or to withhold consent for the use of their personal information, or given an option to opt-out of receiving direct marketing material. It is suggested that individuals must be provided an option to opt-out similar to those under Directive 95/46/EC art 14 (see chapter 5 at [5.2.3.2.3]), and the Spam Act.

The Privacy Act NPPs and the Spam Act both provide opt-out mechanisms in relation to direct marketing. But merely providing information as to their right to opt-out of receiving direct marketing communication or setting out the organisation’s contact details, and/or a

---

number or address so that the recipient can directly contact the sender electronically, places the onus directly on the e-commerce user. A better approach would be to provide express consent through opt-in mechanisms. The Australian Law Reform Commission in its review of the Privacy Act, recommended that the secondary use of personal information should only be possible with express up front consent; if an individual asks not to receive further direct marketing communications, this request must be met within a reasonable period of time; and individuals, on request, should be given information concerning the source of data collected about them. This approach gives greater control to the e-commerce user of their personal information. It allows the e-commerce user to decide whether they wish to receive direct marketing information rather than allowing commercial interests to predominate at the expense of the individual.

In summary, NPP2.1(c) should adopt an opt-in mechanism by requiring prior consent; secondly, organisations should be required to prominently display on the ISP’s or e-business Web site notices which alert the user to the effect of subscribing; thirdly permit the user to ‘unsubscribe’ to the secondary use and/or disclosure of personal information similar to that under the Spam Act; finally, NPP2(iii)–(iv) should be amended to require all senders of direct marketing electronic communications to provide a functional unsubscribe facility similar to that in the Spam Act s 18. These measures will deter unlawful data collection and misuse of personal information by direct marketers and e-businesses and better protect consumers and Internet users against privacy breaches.

6.2.2.3 Access and Correction (NPPs 3, 5, 6)

Under NPP3 ‘Data quality’ principle, an organisation ‘must take reasonable steps to make sure that the personal information it collects, uses, or discloses is accurate, complete and up-to-date’, while under NPP5 ‘Openness’ principle individuals must be provided access to personal information held by an organisation on request, with information on the type of personal information that is held, used and disclosed by the data collector. Individuals

97 Australian Law Reform Commission, Government, above n 2; See also New South Wales Law Reform Commission, above n 97.
98 In addition to the proposal by the Australian Law Reform Commission, above n 2, the New South Wales Law Reform Commission has also proposed that a separate principle for direct marketing should be adopted to apply to organisations that collect personal information for primary purposes or secondary purposes; and that the principle for direct marketing should also distinguish between direct marketing to existing customers and non-existing customers. See New South Wales Law reform Commission, above n 97.
99 NPP5 relate to transparency in information collection. Under NPP5.1 an organisation must set out in a document, clearly expressed policies on its management of personal information and the organisation must
also have the right to have any inaccurate information stored about them corrected.\textsuperscript{100} NPP6 provides for access to and correction of inaccurate information about a data subject.\textsuperscript{101} However, the rights to access and correction are compromised in a number of ways.

First, the duty is not an absolute duty but a duty only to take reasonable steps in relation to the information held. The data subject may be excluded, or may not be allowed to access their personal information. This is especially so when a major part of e-commerce transactions involve trans-border transactions where national laws do not have effect. The problem is that if personal information is collected without consent by ISPs and e-businesses, the data subject will not know if personal information has been transferred from Australia. Besides a lack of consent to such transfers, once their personal information is transferred, individuals may also not have access to and/or be able to correct incorrect information about them. This will mean that the data collector may not be able to comply with NPP3 which requires that reasonable steps be taken to make sure that the personal information which it collects, uses or discloses is accurate, complete and up-to-date.

\textsuperscript{100} Privacy Act 1988 (Cth) sch 3 NPP3, NPP5.

\textsuperscript{101} OECD Guidelines\textsuperscript{[12]} may be viewed as a prerequisite for the Individual participation Principle and it must be possible in practice for the data subject to acquire information about the collection, storage or use of their personal data. See OECD Guidelines\textsuperscript{[12]}. NPP6.4 provides that appropriate transparency and openness requires that access to personal information be provided within a reasonable time, in a reasonable manner, and in a form that is readily intelligible. This is currently required under the OECD Guidelines.
Secondly, as noted earlier, the NPP 6.5 places the onus on the e-commerce user to check to see that the information held is correct. In contrast, the NZ Privacy Act 1993 s 6 places the onus on the agency to check that the information is correct before it is used. All this makes clear that the Privacy Act should provide a process and mechanism that is simple and easy to use, and provide assurance that inaccuracies have been corrected. Furthermore, NPP 6.5 should be amended so that the onus to check to see that the information held is correct should be placed on the organisation that collects personal and sensitive information rather than to shift the onus on the e-commerce user. In relation to the response time for requests for access, the former Privacy Commissioner suggested that if a written request for access is made, the appropriate response time to acknowledge the request should be as soon as possible or at least within 14 days in many cases. It was also suggested that in more complex cases 30 days would be appropriate. But in the absence of mechanisms to ensure prompt response, there can be no assurance that this occurs. As there is no requirement of prior notification under the Privacy Act NPPs, no one actually knows what information is held by data collectors.

### 6.2.2.4 Data Security (NPPs 3, 6, 4)

Data security is fundamental to information privacy. A data security breach may allow unauthorised access to personal and sensitive information about an individual. There have been a number of high profile security breaches which have compromised e-commerce users’ private information. In April 2011, Sony posted an update on its blog and warned its 70 million or so PlayStation Network customers that their personal information had been compromised. There was also a security breach of Heartland Payment Systems that processed major credit cards such as Visa, MasterCard, American Express and Discover card. In the case of Citibank with over 150 million card holders throughout the globe, card holders were only notified of the breach after a considerable delay. Although Citibank

---

102 The OECD’s ‘Individual Participation principle and EC Directive 95/46/EC art 12, places the onus on the organisation to demonstrate that the information is inaccurate.
103 Refer to Australian Law Reform Commission, above n 2, [29.183] 1019.
105 Cf the EU provisions for mandatory notification and informed consent prior to data processing previously discussed in chapter 5 at [5.3.2.3].
replaced the cards, customer details that included name, address, account number, password, and pin numbers were obtained by cyber criminals hacking into Heartland’s database. Although these are examples from other jurisdictions, it may be surmised that similar problems are possible in Australia.

E-commerce users are seldom notified promptly of incidents particularly if there is breach of data security. Data collectors often shift the burden to protect against a security breach to the consumer who is required to take measures to protect their personal information. Banks and other financial institutions now require customers using online banking, credit card transaction or international transactions to ensure that their privacy is not breached when they enter their personal information. If there is any breach of security in relation to PIN numbers or personal identification numbers, then the bank customer is required to provide evidence that care was exercised to protect their PIN from being compromised or exposed to third parties; or that they use the authorised websites. When credit card details in databanks and emails addresses are harvested from the Internet through the use of data mining and surveillance or sold to e-business, often this will be unknown to the individual e-commerce user.\textsuperscript{108}

NPP3 provides for data quality and NPP4 provides for data security. Under NPP4 organisations are only required to take reasonable steps to protect personal information from misuse, loss, unauthorized access, modification or disclosure and to destroy or permanently de-identify personal information if it is no longer needed for any purpose for which the information may be used or disclosed under NPP2.\textsuperscript{109} In addition, NPP6 provides that an organisation is required to take measures to ensure that the personal information that it holds is accurate and up-to-date, and is kept secure from unauthorised use, or access.


\textsuperscript{109} NPP4.1 provides that, ‘an organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure’ and NPP4.2 provides that, ‘an organisation must take reasonable steps to destroy or permanently de-identify personal information if it no longer needed for any purpose for which the information may be used or disclosed under National Privacy Principle 2’.
In contrast to the NPPs, under the Directive 95/46/EC art 17 the provisions relating to data security are mandatory and enforceable.\textsuperscript{110} There is also mandatory provision for data security breach notification.\textsuperscript{111} Australian E-commerce users are entitled to demand that they be promptly notified of a security breach. General guidelines requiring organisations to take appropriate measures are unlikely to be effective and are not directly enforceable. What is required at a minimum is prompt and mandatory notification to the e-commerce user of a data security breach similar to Directive 95/46/EC art 17. Directive 95/46/EC art 6 also requires the data processor to monitor compliance with the requirement.

6.2.2.5 Transborder Data Flows of Personal Information (NPP9)\textsuperscript{112}

Privacy Act, NPP9 provides that:

\begin{quote}
\ldots an organisation in Australia or an external Territory may transfer personal information about an individual to someone (other than the organisation or the individual) who is in a foreign country only if:

(a) the organisation reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the information that are substantially similar to the National Privacy Principles; or
(b) the individual consents to the transfer; or
(c) the transfer is necessary for the performance of a contract between the individual and the organisation, or for the implementation of pre-contractual measures taken in response to the individual's request; or
(d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the organisation and a third party; or
(e) all of the following apply:

(i) the transfer is for the benefit of the individual;
(ii) it is impracticable to obtain the consent of the individual to that transfer;
(iii) if it were practicable to obtain such consent, the individual would be likely to give it; or
\end{quote}

\textsuperscript{110} Refer to chapter 5 at [5.3.2.5].
\textsuperscript{111} The OECD Guidelines - Security Safeguards Principle imposes an obligation on data collectors to maintain confidentiality and ensure the safety of personal information held by them; Articles 6, 18–21 of Directive 95/46/EC also provide for the security of personal information and notification of data security breach.
\textsuperscript{112} See NPP 9 in Appendix 3.
the organisation has taken reasonable steps to ensure that the information which it has
transferred will not be held, used or disclosed by the recipient of the information
inconsistently with the National Privacy Principles.

NPP9 deals with the flow of personal information across borders.\(^\text{113}\) There is an initial
issue of when information can be said to be transferred out of the jurisdiction. The Office
of the Australian Information Commissioner submitted to the Australian Law Reform
Commission (ALRC) that the term ‘transfer’ should be defined.\(^\text{114}\) It is not clear if the term
‘transfer’ captures the transfer of personal information on the internet, emails, and
passwords that are hosted in a foreign country. There is the further problem whether
‘transfer’ should extend to information transferred overseas accidentally particularly where
there has been a breach of data security. NPP9 deals only with transfer to ‘someone’ in a
foreign country. The ALRC recommended that it be amended to refer to transfer outside
Australia to a recipient that would include any agency, organization or individual.\(^\text{115}\) In
addition NPP9 does not make it clear whether a distinction is to be drawn between
‘transfer’ and ‘use’ and ‘disclosure’. The distinction may not be necessary because use and
disclosure are covered by NPP2.\(^\text{116}\) These uncertainties in the operation of NPP9 suggest
that clarification on three matters is required: what qualifies as a transfer; the relationship
to use and disclosure requirements under NPP2 and amendment to refer to transfer outside
Australian to ‘recipients’ rather than ‘someone’.

6.2.2.5.1 ‘Transfer to Related Body’

NPP9 outlines the conditions under which an organisation may transfer personal
information about an individual to someone in a foreign country.\(^\text{117}\) The transfer of
information within the same organisation or to a related body corporate is not technically
subject to NPP9. The related company may be in a jurisdiction which does not have
privacy laws or where the protection of privacy is inadequate. The extra-territoriality
provisions contained in Privacy Act s 5B do not apply to related bodies corporate outside
of Australia.\(^\text{118}\) The Privacy Act s 13B(1) also provides that if a body corporate collects or

---

\(^{113}\) New South Wales Law Reform Commission, above n 97.
\(^{115}\) Australian Law Reform Commission, above n 2, vol 2 [31.175].
\(^{116}\) Ibid, [31.177].
\(^{117}\) Privacy Act 1988 (Cth) sch 3 NPP 9.
\(^{118}\) Ibid, s 5B relates to extra-territorial operation of Act and applies to overseas acts and practices of
organisations. Section s 5B (1) provides that the Act (except Divisions 4 and 5 of Part III and Part IIIA) and
discloses personal information (other than sensitive information) about the individual to a related body corporate,\(^{119}\) it is not an interference with privacy of an individual. The Privacy Act ss 6A (4), 6B (4), 13D (1) also provide that where overseas acts and practices are required by an applicable foreign law, they are generally not considered interferences with the privacy of an individual. The effect is that transfer overseas by an organisation to a related body corporate is not subject to NPP9. Consequently the protections given to Australian e-commerce users under NPP9 are denied to e-commerce users in relation to transfers of personal information out of Australia to a related body corporate.\(^{120}\) Even if the related bodies corporate are governed by a common set of internal policies such policies may not always provide the same level of protection as the Privacy Act. This is the effect of the Privacy Act s 13B (1). So the Privacy Act s 13B should be amended to clarify that if an organisation transfers personal information to a related body corporate outside Australia or to an external territory, the transfer will be subject to the ‘Cross-border Data Flows’ principle’.\(^{121}\) Consequently, the provision should be amended to require related body corporate transfer of information to be subject to NPP9.\(^{122}\) Although this can involve

approved privacy codes extend to an act done, or practice engaged in, outside Australia and the external Territories by an organisation if, (a) subject to subsection (1A), the act or practice relates to personal information about an Australian citizen or a person whose continued presence in Australia is not subject to a limitation as to time imposed by law; and (b) the requirements of subsection (2) or (3) are met. Privacy Act s 6A provides for breach of NNPs, 6B provides for breach of approved privacy code and 13A provides for interference with privacy by organisations. Privacy Act s 5B notes that the act or practice overseas will not breach a National Privacy Principle or approved privacy code or be an interference with the privacy of an individual if the act or practice is required by an applicable foreign law. Privacy Act s 5B (1A) provides that, s 5B (1) (a) does not apply in relation to National Privacy Principle 9. This is because of subsection (1A), the extra-territorial application of National Privacy Principle 9 is not limited by the citizenship etc. requirement of paragraph (1) (a). Section 5B (2) relate to organisational link with Australia. It provides that organisation must be: (a) an Australian citizen; or (b) a person whose continued presence in Australia is not subject to a limitation as to time imposed by law; or (c) a partnership formed in Australia or an external Territory; or (d) a trust created in Australia or an external Territory; or (e) a body corporate incorporated in Australia or an external Territory; or (f) an unincorporated association that has its central management and control in Australia or an external Territory. Under s 5B (3) if an organisations has other link with Australia then all of the following conditions must be met: (a) the organisation is not described in subsection (2); (b) the organisation carries on business in Australia or an external Territory; (c) the personal information was collected or held by the organisation in Australia or an external Territory, either before or at the time of the act or practice. Privacy Act s 5B (4) provides the Australian Information Commissioner with power to deal with complaints about overseas acts and practices. Privacy Act pt V provides for extra-territorial operation so far as that Part relates to complaints and investigation concerning acts and practices to which this Act extends because of subsection (1).This lets the Commissioner take action overseas to investigate complaints and lets the ancillary provisions of pt V operate in that context.

\(^{119}\) A ‘related body corporate’ is ‘a holding company or another body corporate; a subsidiary of another body corporate; or a subsidiary of a holding company of another body corporate; and the mentioned body and the other body are related to each other’; See also the definition of ‘related body corporate’ under Corporations Act 2001 (Cth) s 50 referred to in Privacy Act 1988 (Cth) s 6(8).

\(^{120}\) The gap in protection is not resolved by s 5B dealing with extra-territoriality application. See Australian Law Reform Commission, above n 2, [31.203].

\(^{121}\) Australian Law Reform Commission, ibid, [31.205].

\(^{122}\) Ibid, [31-5]; See also New South Wales law Reform Commission, above n 97, [11.30]-[11.32].
significant costs to related companies, it is a cost which should be regarded as a normal
cost of doing business.

In contrast to NPP9, Directive 95/46/EC art 25 requires that the transfer of personal
information to a third country may only take place if the third country provides assurances
of an adequate level of protection that is assessed on the basis of all circumstances
including the rules of law, both general and sectoral that is in force in the third country in
question. In addition there is the further provision under art 26 which allows the transfer of
information to a non-complying country if adequate safeguards are in place (see chapter 5
at [5.3.2.6]). Article 26 (3), provides that Member States shall provide that a transfer or
a set of transfers of personal data to a third country which does not ensure an adequate
level of protection within the meaning of Article 25(2) may take place on condition that
the transfer is necessary for the conclusion or for the performance of a contract concluded
in the interest of the data subject between the controller and a third party. So it appears
that the EU provision is much stronger in contrast to the provision under NPP9.

6.2.2.5.2 Cross-border transfer to unrelated third parties

Information may be held by offshore businesses or transferred for processing to offshore
facilities. Overseas business processing centres are increasingly handling customer data
in such sensitive areas as credit card applications and bills, mortgage applications,
insurance claims and help desk services. Australian customers’ financial and credit
information is frequently processed by offshore credit reporting companies. Businesses
share information about their customers and suppliers with partners and organisations
linked with their business. A customer’s personal information held by direct marketing
and telemarketing businesses may also be transferred to any branch of an e-business

---

123 Directive 95/46/EC art 2 (f) defines a ‘third party’ to mean a ‘natural or legal person, public authority,
agency or any other body other than the data subject, the controller, the processor and the persons who, under
the direct authority of the controller or the processor, are authorized to process the data’.
124 Marie Schroff, ‘Privacy and Sovereignty: Data Fight or Flight?’ GOVIS 2007 – Innovation in ICT
125 George B Cruchfield and Gaut D Roach, ‘Offshore Outsourcing to India by EU and US Companies: Legal
126 There are organisations that store financial and credit information in foreign jurisdictions. Examples of
organisations that store personal information about customers include overseas but now Australian owned
banks and credit card companies that store customer’s banking details in Australia.
127 Katherine Sainty and Andrew Ailwood, ‘Implications of Transborder Data Flow for Global Business’
company that might store its customer database offshore.\textsuperscript{128} According to some estimates India controls ‘44% of the global outsourcing market of software and back-office services’.\textsuperscript{129} As there is no monitoring of overseas transfers of data, there is no way of knowing how organisations are securing compliance with NPP9 or whether they are exempt because the transfer is to a related corporation, or they are a small business and not bound by the NPPs. Without monitoring, e-commerce users cannot be assured that their private information will be protected. There are also issues related to access and correction where data is transferred out of Australia. If e-commerce users do not know that their personal information is being transferred to a foreign country there is no opportunity to access or verify information transferred. The data may be transferred to a country which does not have adequate privacy protection such as in India and China.\textsuperscript{130}

The extra-territoriality provisions of the Privacy Act are also relevant to the transfer of personal information out of Australia. The Privacy Act s 5B (1) applies to an act or practice engaged in outside Australia and the external Territories by an organisation that relates to personal information about an Australian citizen or a permanent resident\textsuperscript{131} while s 5B (4) provides for the enforcement powers of the Australian Information Commissioner. The Privacy Act s 5B(4), enables the Australian Information Commissioner to hear the complaint if an act or practice relates to personal information about an Australian citizen or permanent resident and either the organisation is linked to Australia by being a citizen; or a permanent resident; or an unincorporated association, trust, partnership or body corporate formed in Australia; or carried on a business in Australia and held or collected information in Australia either before or at the time of the act done or practice engaged in.\textsuperscript{132} The purpose of the provision is to ensure that privacy obligations are not avoided by transfer to third countries who do not have adequate privacy protection for personal information.\textsuperscript{133} The problem, however, is that the transaction may take effect offshore and the provider is not within the jurisdiction. Consequently, it is unlikely that the Australian

\textsuperscript{128} George B Cruchfield and Gaut D Roach, above n 125; Steven Robertson, ‘Offshore Business Processing in China Brings Privacy Concerns’ (2008) 10 Internet Law Bulletin 9,118.
\textsuperscript{129} Nandkumar Saravade and Ponnurangam Kumaraguru, ‘Data Security Council of India - A Self-Regulatory Initiative in Data Security and Privacy Protection’ (2007) 7 Internet Association of Privacy Professionals (‘IAPP’) 11. The total revenue due to IT and business process outsourcing in India is expected to grow to $60 billion by 2010 and China is beginning to ‘rival the outsourcing powerhouse, India’. See Steven Robertson, above n 129, 118; Australian Law Reform Commission, above n 2.
\textsuperscript{130} George B Cruchfield and Gaut D Roach, above n 125.
\textsuperscript{131} Privacy Act 1988 (Cth) s 5B (1).
\textsuperscript{132} Ibid, s 5B (2).
\textsuperscript{133} Australian Law Reform Commission, above n 2 [31.72].
Information Commissioner will take up and investigate a complaint by an individual e-commerce user and even if the Commissioner did there is no readily available means of enforcement. The enforcement of the NPPs is discussed in chapter 8 at [8.4.1].

6.2.2.5.3 The issue of consent under NPP9

Under NPP9, an e-commerce user may consent to the transfer of personal information overseas.\textsuperscript{134} This may be perfunctory and uninformed (see chapter 4 at [4.2]). However, an e-commerce user’s consent is not mandatory for transfer. NPP9 allows the transfer without consent if the transfer is for the benefit of the individual, and it is impracticable to obtain consent of the individual to the transfer; and/or if it were practicable to obtain such consent, the individual would be likely to give it; and if the organisation transferring such information has taken reasonable steps to ensure that the information transferred will not be held, used or disclosed by the recipient inconsistently with the NPPs. However, since there is no monitoring of this data transfer it is difficult to ascertain whether there is compliance with NPP9.\textsuperscript{135} As previously mentioned above, there is no mandatory requirement for notification prior to the collection of personal information under the Privacy Act (see above at [6.2.2.1]).

There is relatively weak protection under NPP9 (a), (f) which allows the transfer of personal information without consent if:

(a) the organisation reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the information that are substantially similar to the National Privacy Principles;

(f) the organisation has taken reasonable steps to ensure that the information which it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with the National Privacy Principles.

In comparison to Directive 95/46/EC (see chapter 5 at [5.3.2.6]), NPP9 appears to be deficient in a number of respects: (1) the organisation transferring data is not accountable for any subsequent breaches; (2) the standard required of ‘reasonable belief’ in NPP9 (a)

\textsuperscript{134} Refer to Privacy Act 1988 (Cth) NPP9 (b) in Appendix 3.

does not require verification or other measures to better protect personal data; (3) the
operation of consent in the context of transborder data flows is not mandatory; (4) a lack of
clarity as to how NPP9 relates to other parts of the Privacy Act; and (5) a lack of guidance
for organisations as to what steps they must take to comply with NPP9.

In relation to NPP9, it contrasts with the very strong measures put in place by the EU to
protect its citizens. First, Directive 95/46/EC requires prior approval for collection of
personal information together with details of proposed disclosure and usage. Notification
of cross-border transfer is one element in the effective protection against inappropriate
transfer of personal information overseas (see chapter 5 at [5.3.2.6]). Secondly the EU
provides a formal process for deciding whether a third country provides comparable
protection. Directive 95/46/EC, art 20 provides that if the processing of personal data is
carried out by a person established in a third country, prior checks must be made by the
Supervisory Authority in the Member State to determine if there is likely to be specific
risks to the rights and freedoms of the data subject following the receipt of notification of
the processing of personal data. Moreover, Directive 95/46/EC art 25(4) provides that
where there is not an adequate level of protection, EU Member States must take necessary
measures to prevent transfer. This is subject to exceptions contained in Directive 95/46/EC
art 26 (1) (see chapter 5 at [5.3.2.6]). Where a country does not meet this standard,
Directive 95/46/EC further provides standard form contractual provisions which
incorporate privacy policy statements and privacy codes (see chapter 4 at [4.2.2]; chapter 5
at [5.3.2.6]) and give a private right of action to EU citizens for breach. The use of
standard form contractual clauses for the transfer of personal data to a non-compliant third
country provides one solution to ensure accountability, and still facilitate the transfer of
personal data. These measures give a greater level of protection to EU citizens than do
the Australian provisions. Another alternative adopted by Canada is to impose
responsibility directly on the organisation that has collected the information. The

It should be noted that the Australian privacy legislation and the NPPs do not meet the adequacy test for
these purposes, see chapter 5 at [5.3.2.6]; see also European Commission, Commission Decisions on the
European Commission, Agreement between the European Union and the United States of America on the
Processing and Transfer of Passenger Name Record (PNR) Data by Carriers to the United States
Department of Homeland Security (DHS), (23 July 2007).

Commission Decision 2002/16/EC art 3, defines a ‘data exporter’ means the controller who transfers the
personal data and ‘data importer means the processor established in a third country who agrees to receive
from the data exporter personal data intended for processing on the data exporter’s behalf after the transfer in
accordance with his instructions and the terms of this Decision and who is not subject to a third country’s
system ensuring adequate protection within the meaning of EC Directive 95/46/EC, art 25 (1)’.
organisation remains responsible for privacy breaches by a third party processing the information that follow the OECD’s accountability principle (see chapter 5 at [5.2.1.5]). It requires the organisation to ‘use contractual or other means to provide a comparable level of protection while the information is being processed by a third party’.

NPP9 does not, like the EC’s Directive 95/46/EC, establish standard enforceable clauses guaranteeing the privacy of EC citizens where personal information is held, used or disclosed in a third country. Even if privacy laws on the face of it provide equivalent protection there is no guarantee that they are sufficiently enforceable where personal data is transferred to a third country.

The Australian Law Reform Commission (ALRC) has in its recent review of the privacy laws recommended a set of Unified Privacy Principles (UPPs) for consistency across all Australian jurisdictions. The fair information principle for transborder flows of personal information is contained in the recommended UPP11. UPP11–Cross-border Data Flows provides that:

[I]f an agency or organisation in Australia or an external territory transfers personal information about an individual to a recipient (Other than the agency, organisation or the individual) who is outside Australia and an external territory, the agency or organisation remains accountable for the personal information, unless the:

(a) agency or organisation reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds privacy protection that are substantially similar to these principles;

(b) individual consents to the transfer, after being expressly advised that the consequence of providing consent is that the agency or organisation will no longer be accountable for the individual’s personal information once transferred; or

---

139 Australian Law Reform Commission recommended a set of uniform privacy principles. See also New South Wales Law Reform Commission, above n 97.
(c) agency or organisation is required or authorized by or under law to transfer the personal information.\textsuperscript{140}

In addition the ALRC has recommended that the federal Australian Information Commissioner should develop and provide guidance on the ‘Cross-border Data Flows’ principle (Unified Privacy Principle (UPP) 11). These guidelines follow the EC approach by recommending the development of model contractual terms dealing with the transfer of personal information to recipients outside Australia.\textsuperscript{141} It should require that individuals expressly consent to the transfer after being expressly notified of the destination jurisdiction/s of the transfer and the likelihood of further transfer; the intended recipient/s; and the intended users if known; and the consequences of providing consent is that the agency or organisations will no longer be accountable for the individuals’ personal information once transferred.\textsuperscript{142} However, the consent exception under the proposed UPP11 is more restrictive that that provided under NPP9 as it requires that individuals be expressly advised of the consequences of providing consent.\textsuperscript{143}

Although the recommended new UPP principles give greater protection to Australian e-commerce users’ personal information, they continue to fall short of the superior protection under the EC provisions. Particularly as there is no formal process for ensuring that the laws of another country are in fact equivalent to the protection available for e-commerce users in Australia. International organisations and businesses that operate globally may also not be certain as to the applicable law, jurisdiction and oversight.\textsuperscript{144} The transborder flows of personal data continue to be a source of community concern. A survey commissioned by the then Office of the Privacy Commissioner reveal that 90% of those who responded to the survey were concerned about businesses sending their personal information overseas, 63% were very concerned.\textsuperscript{145}

\textsuperscript{140}New South Wales Law Reform Commission, above n 97 [11.1].
\textsuperscript{141}Australian Law Reform Commission, above n 2 [31.230], Recommendation 31-7(c).
\textsuperscript{142}New South Wales Law Reform Commission, above n 97.
\textsuperscript{143}It provides: ‘[the] individual consents to the transfer, after being expressly advised that the consequence of providing consent is that the agency or organisation will no longer be accountable for the individual’s personal information once transferred.’ See Australian Law Reform Commission, above n 2, [31.242] 1129.
6.3 Conclusion

This Chapter has examined Australia’s regulatory approach to information privacy protection under the Privacy Act and related NPPs. It concludes that the Privacy Act and related NPPs fail to give adequate protection to e-commerce users’ rights to privacy as compared to those provided for example under the Directive 95/46/EC. Commercial interests, efficiency and cost have been given priority over personal privacy. Indicative of this is the exemption of small businesses; except in relation to sensitive information, businesses are not required to obtain consent of the individual nor approval from a supervisory authority before collection, use or disclosure of personal information. Privacy protections are couched in the language of efficiency. So, for example, protection extends to individuals who are ‘reasonably ascertainable’ which inevitably draws on cost considerations. Similarly cross border protection for information transferred without consent depends upon ‘reasonable belief’ that information will be protected in an offshore environment. The NPPs do not require that consent of an e-commerce user be appropriately informed by readily accessible and available material. The onus is placed on e-commerce users to take steps to protect their privacy so that there are opt-out mechanisms rather than opt in mechanisms. Direct marketing is permitted without the e-commerce users’ consent.

In contrast, this chapter highlighted the superior protection provided under Directive 95/46/EC which requires prior registration and notification to the respective supervisory authority before the collection of personal information and notification to the individual affected (see chapter 5 at [5.3.2.3]). The Privacy Act NPPs 1, 10, 2 should be amended to require prior registration with the supervisory authority and that data subjects must be notified prior to collection, use and disclosure of their personal information.

The protection of privacy requires that the individual e-commerce user is sufficiently informed prior to waiving privacy rights. In order to achieve this, the Privacy Act should provide specific guidelines on what information a commercial websites or online services should post on their online web site in relation to their privacy policies.146 These policies

---

146 See Online Privacy Alliance, ‘Guidelines on Privacy Policies’ (2010) for a detail discussion on the elements and the posting of privacy policies on online web sites by commercial entities involved in data collection, use and disclosure, and the sharing of personal information with their commercial partners. See
should be in easily understood language and easily accessible (see chapter 4 at [4.2.1]; [4.2.1.1]). The difficulties are not limited to the collection, use and disclosure of personal information but rapid notification where there has been a security breach. The failure of Australian privacy legislation and NPPs to require these measures gives preference to commercial interests over privacy interests.

In its review of the Privacy Act, the ALRC Report 108 made 295 recommendations to improve personal information privacy protection. A key recommendation was the adoption of a set of unified principles (Uniform Privacy Principles) governing both the public and private sector. Although the legislative implementation of these recommendations would remove some of the key objections to the current legislative framework, they do not go as far as the EC principles in protecting individual privacy. The major omissions relate to prior registration with a supervisory authority and tighter control over cross border privacy issues.

The Privacy Act should ensure that the collector of personal information remains accountable for the handling, disclosure and use of that information with appropriate enforcement mechanisms. It will be apparent from chapter 8 dealing with enforcement that the Australian provisions relating to enforcement are extremely weak in comparison with the provisions under Directive 95/46/EC.

The Privacy Act, NPPs do not apply where there is an authorised industry code. The following chapter 7 will discuss industry regulation through codes of practices in Australia.


147 See Australian Law Reform Commission, above n 2.
Chapter 7: Industry Privacy Codes

7.1 Introduction

The previous chapter examined Australia’s framework for information privacy protection under federal legislation. This chapter examines the development of industry privacy codes both under the Privacy Act and under specific federal legislation.

The Australian Information Commissioner (‘AIC’) has power under the Privacy Act to approve industry privacy codes of practice. In addition to the Australian Information Commissioner, there are other regulators that have the power to approve industry codes of practice related to privacy under other federal legislation, including the Australian Securities and Investment Commission (hereafter referred to as ‘ASIC’) and the Australian Competition and Consumer Commission (hereafter referred to as ‘ACCC’). In relation to the telecommunications industry, the code regulator is the Australian Communications and Media Authority (hereafter referred to as ‘ACMA’). In considering the development and approval of industry privacy codes, this section points to the problems created by a multiplicity of regulators who have a role to play in the formulation, approval and supervision of industry codes.

The focus in this chapter is on approved industry codes under the Privacy Act and those industry codes that are related to e-commerce in the Telecommunications sector: the Telecommunications Consumer Protection (TCP) Code (hereafter referred to as ‘TCP Code’),¹ and the Australian E-Marketing Code of Practice (hereafter referred to as ‘e-Marketing Code’).² The TCP Code and the e-Marketing Codes are developed under Telecommunications Acts 112 and s112 (1A) respectively.

7.2 Industry Codes

Generally industry regulation is characterised by industry formulated rules and codes of practice. In relation to privacy protection for e-commerce users, industry codes are not a matter left exclusively to the industry to determine. The Privacy Act provides that

---


approved industry codes may substitute for the NPPs discussed in the previous chapter. There is, in addition, provision for codes in relation to a particularly important small segment of the e-commerce market that is the telecommunications industry. It is to be noted that compliance with an industry code under the Telecommunications legislation is voluntary unless the ACMA directs a particular participant in the telecommunications industry, the e-marketing industry, the telemarketing industry, or the fax marketing industry to comply with the code.\(^3\) The emphasis in this chapter is on approved industry codes under the Privacy Act and approved codes under the Telecommunications Act that relate to e-commerce.

### 7.3 Privacy Act - NPPs

The ten NPPs examined in chapter 6 at [6.2.2], set minimum standards for the collection, use and/or disclosure, access and correction of personal information.\(^4\) It should be noted at the outset that the NPPs provide default rules applying to non-exempt organisations where there is no applicable approved industry code.\(^5\) Under the Privacy Act pt. IIIAA, an organisation or industry sector may develop privacy codes that can operate in place of the legislative framework.\(^6\) These codes are binding on industry members and substitute for the NPPs.\(^7\) The Privacy Act s 6EA allows exempt groups to opt to comply with the NPPs but very few have done so. Currently there are three industry codes of practice that have been approved and registered under Privacy Act by the former Office of the Privacy Commissioner (now the Office of the Australian Information Commissioner (‘OAIC’)). These are: the Market and Social Research Privacy Code; Queensland Club Industry Privacy Code; and Biometrics Institute Privacy Code.\(^8\) This suggests that industry does not see any special benefit in developing its own codes of practice. There are, in addition, industry codes developed under Telecommunications and other legislation (see below at

\(^3\) Telecommunications Act 1997 (Cth) s 5.

\(^4\) Refer to Privacy Act 1988 (Cth) NPPs in Appendix 3.

\(^5\) Privacy Act 1988 (Cth) s 16A provides that organizations must comply with approved privacy Codes or NPPs.


\(^7\) A co-regulatory scheme involve industry and government regulation where codes of conduct that is provided through specific legislation. For more details on the various regulatory models subscribed to in Australia and elsewhere, see Australian Government, Task Force on Industry Self- regulation, The Treasury, ‘Appendix D: International Policy on Industry Self-regulation’ (Australian Government, 2000).

[7.5]) and voluntary codes of practice such as the Direct Marketing Code of Practice developed by the Australian Direct Marketing Association (‘ADMA’) for the direct marketing industry.\(^9\)

Any organisation, group of organisations, or any industry organisations that is exempt or non-exempt under the Privacy Act can make an application to the Australian Information Commissioner to have a privacy code approved.\(^10\) This allows the development of specific industry codes of practice to allow flexibility of application for organisations.\(^11\) Under the Privacy Act s18BB, the Australian Information Commissioner may approve a privacy code only if the Commissioner is satisfied that: the code incorporates all NPPs or sets out obligations or the equivalent of all the obligations set out in the NPPs; specifies organisations that are bound or will be bound by the code; only organisations that consent are bound by the code; the code sets out a procedure for organisations to cease to be bound; and making and dealing with complaints that may be an interference with the privacy of an individual under the Privacy Act. The Australian Information Commissioner must also be satisfied that members of the public have had an adequate opportunity to comment on the draft code. Moreover, under the Privacy Act s18BF, the Australian Information Commissioner can issue binding and non-binding guidelines\(^12\) for developing privacy codes which the Commissioner approves.\(^13\)

### 7.4 Supervisory Authorities and Code Regulators

Besides the Australian Information Commissioner, the ACMA, the Telecommunications Industry Ombudsman (hereafter referred to as ‘TIO’) and other industry regulators such as

---


\(^10\) See Office of the Privacy Commissioner, Code Development Guidelines and Information Sheet 11-Privacy Codes (2001). Organisations may apply for approval of a code under Privacy Act 1988 (Cth) s18BA.

\(^11\) Privacy Act 1988 (Cth) s18BB. Section 6EA also allows small businesses to opt in and to be subject to the NPPs.

\(^12\) Privacy Act 1988 (Cth) ss 27(1) (p), 27(1) (pa), 95AA; See Office of the Privacy Commissioner, ‘Revised Version of the Code Development Guidelines’ (2001).

\(^13\) Privacy Act 1988 (Cth) s18A(1) (a)-(d). The Australian Information Commissioner must by notice publish in the Gazette, the issue of a Code of Conduct concerning the collection, storage of, security of, access to, correction of, use and disclosure of personal information included in the credit information files or in credit reports.
the ASIC (the corporate regulator), and the ACCC (the regulator for competition and consumer protection) also regulate industry codes.

The point here is that at the federal level there is a maze of different regulators and code supervisors who may have some role to play in relation to privacy breaches involving e-commerce users. There may be an advantage to having multiple bodies with specialist industry expertise that are responsible for a particular sector such as telecommunications privacy. This may have the incidental effect of reducing the volume and burden of privacy complaints to the Australian Information Commissioner thus freeing resources for other complaints. However, the considerable overlap between the roles played by regulators with the differing approaches fails to provide a consistent and coherent approach viewed from the perspective of the individual e-commerce user. The existence of multiple regulators in the telecommunications industry confuses consumers making complaints about telecommunications privacy issues, and wastes agency resources. The handling of complaints by multiple bodies also gives rise to a lack of jurisdictional clarity, possible delay and complicates investigation of complaints, with astute consumers engaging in forum shopping for the best outcome. In relation to the telecommunications industry, the regulatory roles of the ACMA, the TIO, and the Australian Information Commissioner discussed below should be clarified. The simplest solution is to have a single body responsible for receiving complaints and monitoring and enforcing privacy standards and codes. However, at present the OAIC lacks the resources to deal with telecommunications privacy matters. Moreover political pressures may become more


16 The ALRC has noted that multiple bodies with responsibility for privacy complaints regime result in confusion for consumers, a loss of confidence in the ability of industry regulators to handle complaints effectively, delays in the resolution of complaints, increased costs, duplication of effort by regulators, and forum shopping. See Australian Law Reform Commission, Review of the Australian Privacy Law, DP 72 (2007), [64.119]-[64.126].

17 See Australian Law Reform Commission, above n 16; See also Australian Law Reform Commission, above n 15, [73.203]-[73.205].

18 See the Australian Law Reform Commission, above n 16, [64.119]-[64.126]; See also Australian Law Reform Commission, above n 15, [73.203]-[73.205].
focussed with a single regulator and there remains, as with any other regulator, the issues of accountability and consistency.\textsuperscript{19} This section now turns to look in greater detail at these other supervisory authorities and code regulators.

7.4.1 The Australian Securities and Investment Commission (‘ASIC’)  

ASIC as the corporate regulator has power under s1101A of the Corporations Act 2001, to approve voluntary industry codes of conduct; it does not have the power to mandate industry codes. Instead, it is for an Industry to decide in the first instance whether to develop a code, and then whether to have that code approved by ASIC. Industry codes of practice regulated by ASIC include the Code of Banking Practice, Building Society Code of Practice, Credit Union Code of Practice, and the Electronic Funds Transfer Code of Conduct (EFT Code of Conduct).\textsuperscript{20} Although ASIC is the code regulator, it generally cannot take enforcement action if a code is breached unless a breach of the law is also involved. But if there is significant non-compliance with an industry code, then ASIC may publicise the breach in some instances.\textsuperscript{21}

In relation to those codes which ASIC has power to approve, there is potential for considerable overlap as the Privacy Act extends to consumer credit reporting and consumer credit records. Organisations involved in the provision of credit, the collection and disclosure of consumer credit records are bound by the NPPs and the privacy restrictions in relation to the use and disclosure of credit reports in the Privacy Act Part IIIA.\textsuperscript{22}

The problem for e-commerce users is the confusion about what rules apply, what regulatory authority is responsible for compliance, and whether the NPPs or the relevant Code provides remedies. So, for example, the NPPs are reinforced in the Credit Union

\textsuperscript{19} Refer to Australian Law Reform Commission, above n 15, [46.11].
\textsuperscript{22} Australian Law Reform Commission, above n 15, 1721–1737.
Code generally and the EFT Code in respect of electronic transactions. EFT Code pt C cl 21 relates to privacy and the confidentiality (pt C cl 22) of customer’s account details. The EFT Code, cl 21.1 provides that Code subscribers that subscribe to the EFT Code can either comply with the NPPs or with the Codes where the provider is a subscriber to an approved Code. The EFT Code cl 21.2 provides guidelines to interpret the NPPs and any Code approved by the Australian Information Commissioner referred to above at [7.3]. With respect to confidentiality of transactions, EFT Code cl 21.2 (a) provides that if surveillance devices (visual, sound or data recording) are used by or on behalf of the account institution to monitor EFT transactions, then the account institution or stored value operator must notify the users of such surveillance devices before the commencement of each transaction, or each session of the transaction that the transaction may be recorded by surveillance devices and the nature of the surveillance. EFT Code cl 21.2 (d) provides that if EFT transactions can be conducted through an account institution’s electronic address (such as a website), the account institution should ensure that privacy policies are made available at or through that electronic address and can be provided to a user by electronic communication if the user so requests.  

7.4.2 Australian Competition and Consumer Commission (‘ACCC’)

Industry codes of practice related to online shopping and trading are required to comply with the Competition and Consumer Act, the Privacy Act (including the NPPs), the Telecommunications Act, and the Spam Act. The Competition and Consumer Act 2010 (Cth) provides for industry codes of practice in Part IVB. The ACCC is the primary regulator under s51AE of the Competition and Consumer Act 2010 and responsible for administering industry codes of practice prescribed by law. ACCC regulates mandatory industry codes and monitors compliance with self-subscribed industry codes. There are both mandatory and voluntary codes under the Act. A prescribed mandatory industry

---

24 Formerly known as the Trade Practices Act 1974 (Cth).
25 Competition and Consumer Act 2010 (Cth) pt IVB s 51.
26 Competition and Consumer Act 2010 (Cth) pt IVB div 1 s 51ACA-51AEA; Part IVB provides for Industry Codes; s 51AD provides for contravention of industry codes; s 51ADA, provides that ACCC may issue a public warning notice it has reasonable grounds to suspect a contravention of an applicable industry code by the corporation; pt VI s 75B provides for enforcement; and s 76 provides for remedies.
27 Competition and Consumer Act 2010 (Cth) s 51AE provides that the regulation prescribing an industry code or specified provisions of an industry code may declare the industry code to be mandatory or a voluntary industry code.
code is binding on all industry participants. The only mandatory code relevant to e-commerce users’ privacy is the e-Marketing Code of Conduct. The e-Marketing Code of Practice relates to online marketing. This is examined below at [7.5.2] and in relation to complaints handling, compliance, enforcement, and remedies and sanctions under the Code in chapter 8. Voluntary codes of practice may be prescribed under legislation such as the Competition and Consumer Act 2010 (Cth) but a voluntary code is only binding on those members of an industry or profession who are signatories to the code. There are currently no prescribed voluntary codes under the Act.  

There is substantial scope for overlap between industry codes dealing with privacy and the NPPs. In relation to compliance with the NPPs and privacy codes, under a memorandum of understanding, the ACCC matters related to privacy breaches to the Information Commissioner. This MOU allows appropriate liaison between the ACCC and the Australian Information Commissioner where there are overlaps between the jurisdiction of the ACCC and the Australian Information Commissioner. In relation to the telecommunications industry, besides the ACMA, the ACCC also monitors the telecommunications sector for breach of the Competition and Consumer Act in relation to their dealings with goods and services provided to telecommunications users.

In some situations, three different regulators may be involved in dealing with a privacy issue. The Australian Information Commissioner, ACCC and ACMA, who have overlapping roles so that a data security breach may involve all three regulators (see below). Although protocols and agreements may provide mechanisms for dealing with these overlapping powers, this lack of jurisdictional clarity points to the lack of a coherent approach to privacy protection and problems for e-commerce users in seeking to protect their private information.

---

28 Prescribed voluntary codes of practice are distinguished from non-prescribed voluntary codes of practice. Non prescribed voluntary codes such as the Australian Direct Marketing Code of Conduct arise from an industry initiative and are administered by the industry itself. See Australian Competition and Consumer Commission, ‘Industry Codes of Conduct’ (Date accessed 12 August 2012) http://www.accc.gov.au/content/index.phtml/itemId/783097#h2_17

29 Office of the Privacy Commissioner, ‘Regulators Co-Operate to Improve Privacy Compliance’, Media Release (12 March 2002). A Memorandum of Understanding was signed on 12 March 2002 by the ACCC with the federal Privacy Commissioner which set out the framework in which the two agencies intend to co-operate. The framework included amongst others a regular exchange of information, assisting each other with investigations, and forming a joint task force to conduct litigation.

30 For example issues involving data security and Telstra and Vodafone, see chapter 8 [8.2.2.1]; see also Australian Communications and Media Authority (ACMA), ‘ACCC and ACMA to work together on industry data collection’ Media Release MR 86/2006 (16 August 2006) <http://www.acma.gov.au/WEB/STANDARD/pv=AC-100712>.
7.4.3 Australian Communications and Media Authority (‘ACMA’)

The ACMA has an important role in general consumer protection with respect to the telecommunications industry where there are breaches of the Telecommunications Act pt 13 (see below at [7.5.1]). The ACMA is responsible for the regulation of broadcasting, the Internet, radio, and telecommunications. The Telecommunications Act establishes a multi layered complaints process starting with the provider and concluding with an industry established dispute resolution scheme (see below at [7.4.4]). Currently the enforcement of the Telecommunications Act is delegated to ACMA which is the Industry code regulator. The Act empowers the ACMA to monitor, set standards, and report significant matters on the performance of carriers and carriage service providers to the Minister.  

A telecommunications industry Code must be registered with the ACMA.  

The Telecommunications Act pt 6 s 113 provides for matters that may be dealt under the Act under industry codes and industry standards. These include privacy and the protection of personal information; the intrusive use of telecommunications by carriers or service providers; the monitoring of communications; and calling number display; and provision of directory products and services.

Besides the Telecommunications Act, the Spam Act provides for the ACMA to be the regulator under that Act. As the e-marketing code is established under the Spam Act, the ACMA can enforce compliance with the e-Marketing Code on all members of the e-marketing industry. This covers all persons, individuals and organisations undertaking an e-marketing activity within the meaning of the Spam Act. The ACMA has power to regulate and enforce the Spam Act by imposing financial penalties and sanctions. Under the Spam Act, the sanctions and penalties are substantial when compared with those under the Privacy Act.

In addition to the Spam Act, the Do Not Call Register Act 2006 (Cth) also establishes the ACMA as the statutory regulator and administrator for the industry.

---

31 Telecommunications Act 1997 (Cth) s 5. Compliance with and enforcement of industry Codes will be examined in chapter 8 at [8.3.2].
32 The Australian Communications and Media Authority (‘ACMA’) was established under the Telecommunications Act 1997 (Cth) on 1 July 1997 after the merger of the Australian Broadcasting Authority (ABA) and the Australian Communications Authority (ACA) formerly known as Austel.
33 Telecommunications Act 1997 (Cth) s 113 (f).
34 Spam Act 2003 (Cth) s 26 provides that ACMA may institute proceedings in the Federal Court on behalf of the Commonwealth of Australia for a contravention under the Spam Act 2003 (Cth).
35 See Spam Act 2003 (Cth) ss 24-30 for penalties for breach of the Spam Act 2003 (Cth). Section 25 provides for a maximum penalty of $1.1 Million per contravention that is for every non-compliant message sent.
36 Hereafter referred to as ‘Do Not Call Register Act’.
Code of practice related to the telecommunications and marketing industry. Under s 13 of
the Do Not Call Register Act, the ACMA must keep a Do Not Call Register or arrange for
another person (the contracted service provider) to keep a register of telephone numbers.

Besides the ACMA, several other regulatory bodies are also involved in the regulation of
the telecommunications industry. The TIO plays an important role in monitoring industry
codes that relate to ecommerce. Its powers are derived from the Telecommunications Act,
which is examined next.

7.4.4 Telecommunications Industry Ombudsman (TIO)

The TIO is an independent dispute resolution provider and can investigate complaints
relating to the telecommunications providers and ISPs.37 The TIO is established under pt 6
of the Telecommunications (Consumer Protection and Services Standards) Act 1999 (Cth)
(TCPSS Act). Sections 126-133 of the Act require all licensed providers in the
telecommunications sector to be members of the Telecommunications Industry
Ombudsman (‘TIO’) scheme, 38 and provides for the TIO to investigate, make
determinations and give directions relating to complaints about carriage services by end
users of those services.39 The TIO can also investigate and determine complaints relating
to a breach of an industry code by telephone or internet service providers and also
investigate and determine complaints requiring payment of compensation for costs
incurred for serious breaches of privacy.40 TIO scheme members are required to comply
with TIO determinations under clause 6.1 of the TIO constitution.

The TIO also has powers and functions conferred by industry codes. 41 The
Telecommunications Act pt 6 s 117(1)(j) also provides that where the telecommunications
industry code involves privacy issues,42 the industry body must satisfy the ACMA that the

38 Telecommunications (Consumer Protection and Services Standards) Act 1999 (Cth) (TCPSS Act) provides
that certain carriers and carriage service providers must enter into the Telecommunications Industry
Ombudsman scheme, (s 126); Membership of the scheme must be open to all carriers and carriage service
providers, (s 130); It is required that carriers and carriage service providers must comply with the scheme, (s
132). Exceptions apply under Telecommunications (Consumer Protection and Service Standards) Act 1999 s
129, and it provides that ACMA can declare under s 129, that eligible service providers are exempt from
compliance with the Telecommunications Ombudsman Scheme provided under s 128 (1) of the Act.
41 Telecommunications Act 1997 (Cth) s 6, s 114.
42 Privacy issue as defined in Telecommunications Act 1997 (Cth) s 113(3) (f).
Australian Information Commissioner has been consulted and has approved the privacy code. The Telecommunications Act also requires that ACMA be satisfied that the TIO has been consulted about the development of an industry code prior to it registering the industry Code.\textsuperscript{43} ACMA and TIO have close co-operation with the Office of the Australian Information Commissioner and the ACCC. The ACMA and the TIO have also signed a Memorandum of Understanding with the then federal Privacy Commissioner and the ACCC on 25 March 2008 to promote co-operation between the two agencies.\textsuperscript{44} The consequence is that the approval, regulation and monitoring of privacy codes involves multiple agencies. Although there is provision for consultation, it makes more difficult the effective monitoring of privacy codes.

Here again, the problem posed by multiple regulators must be noted. Besides the Privacy Act, at any one time there are possibly three regulators (i.e. the Australian Information Commissioner, the ACMA, and the TIO) assessing if there is compliance with either the TCP Code (the code is referred to below) or the e-Marketing Code. This approach leaves open the potential for inconsistent approaches to the protection of privacy and enforcement. For the e-commerce user, it adds to the confusion about who should be approached where there is an infringement of the individual’s privacy and dissatisfaction where there is differential enforcement by different bodies. It provides a powerful argument for a single body protecting and enforcing the e-commerce user’s right to privacy.

The Diagram 7.1 set out below illustrates the problem of different regulators with different jurisdictions and powers of enforcement.

\textsuperscript{43} For more details on the powers and function of the Telecommunications Industry Ombudsman see TIO’s Annual Report 2010.

\textsuperscript{44} Australian Communications and Media Authority, ‘ACMA and TIO Signal Closer Co-operation on Complaints, Compliance and Enforcement’, Media Release: 29/2008 (25 March 2008).
The next section examines sector specific telecommunications industry codes of practice that have privacy codes approved by the industry regulator.

### 7.5 Telecommunications Industry Codes of Practice

The Telecommunications Act provides for industry Codes for the telecommunications industry. This is set out under Telecommunications Act pt 6. Telecommunications Act pts 26-28 provide for investigations, information-gathering powers, and enforceable undertakings respectively.\(^{45}\) In relation to consumer’s information privacy, the Telecommunications Act s 112 provides that the telecommunications industry can develop codes that apply to all those involved in the telecommunications industry. The Telecommunications Act s 113(3)(f) provides examples of matters that may be dealt with by the development of an industry code of practice such as disclosure and/or use of

\(^{45}\) See note to Spam Act 2003 (Cth) s 3 which makes reference to the Telecommunications Act 1997 (Cth) pt 6 (industry codes and standards), pt 26 (investigations), pt 27 (information-gathering powers) and pt 28 (enforcement).
information gathered in the course of providing services to customers. The Telecommunications Act s116A provides that:

... neither an industry code nor an industry standard derogates from a requirement made by or under the Privacy Act 1988 or an approved privacy code (as defined in that Act).

So a telecommunications industry code that incorporates a privacy code must provide rules and principles that comply with the national privacy principles (NPPs) for collection, use and disclosure, access and correction, data quality and data security. Consequently the NPPs provide the overriding privacy standards. The Privacy Act s 27(1), the Australian Information Privacy Commissioner has the power (and if the Commissioner considers it appropriate) to investigate an act or practice of an organisation that may be an interference with the privacy of an individual.\(^{46}\)

The Telecommunications Act s 117 requires the code to be submitted to the ACMA for registration. Under s 117(1)(j)-(k) if the code deals with privacy matters, the ACMA must be satisfied that an industry code meets the statutory criteria set out in Privacy Act s 18BB(2). This requires prior consultation by the industry body and the ACMA with the Information Commissioner before a code is approved. Consequently, the approach adopted federally is to provide consultative mechanisms to ensure that the standards set by the Privacy Act set the minimum standards. It may be observed that this results in an inefficient system of regulation.

The next section examines two industry codes of practice. These are the TCP Code under the Telecommunications Act,\(^{47}\) and the Australian e-Marketing Code of Practice 2005 (‘e-Marketing Code’) under the Spam Act that relate to e-commerce and the telecommunications sector. These two codes of practice comply with the minimum requirements of the NPPs (see above in at [7.3.2]), and are regulated by the ACMA, and the TIO. The TCP Code and the e-Marketing Code provide illustrations of industry codes tailored to the needs of the industry but which meet the minimum standards required under the NPPs. The effectiveness and enforcement of the dispute resolution mechanisms under these codes is examined in chapter 8 at [8.4.2].

\(^{46}\) Privacy Act 1988 (Cth) s 27 (1)(ab)-(ae).
\(^{47}\) Telecommunications Act 1997 (Cth) pt 6.
7.5.1 Telecommunications Consumer Protections (TCP) Code (‘TCP Code’)

Part 13 of the Telecommunications Act ss 276-278, regulates the privacy of communications within the telecommunications industry. The TCP Code established under the Telecommunications Act pt 6 regulates telecommunications companies. The TCP Code was developed in 2007 to replace six existing Codes registered with the Australian Communications Industry Forum (ACIF). The TCP Code cl 1.3 provides that the Code applies only to those involved as Carriage Service Providers in the telecommunications industry that provide telecommunications services to residential and small business customers, and to those activities relating to the customer’s relationship with their Carriage Service Providers.

The Telecommunications Act pt 13 provides privacy protection in relation to the collection, use, and disclosure of customer’s telecommunications, personal information or documents. It applies much more broadly than the Privacy Act. Protection extends to include telephone numbers, the time of the call and its duration, postal addresses, and internet based applications including IP addresses for the session and the start and finish time of each session. These may not be covered under the Privacy Act (see chapter 6 at [6.2.1.3]). In contrast to the Privacy Act and the NPPs, the TCP Code which derives from the telecommunications legislation, also covers a much wider scope of personal information about a customer including billing and related personal information (see chapter 6 at [6.2.1). The TCP Code cl 6.8 provides that a telecommunications industry supplier must protect the privacy of each customer's billing and related personal information.

---


49 These include the Customer Information on Price, Terms & Conditions Industry Code (ACIF C521, 2004); the Credit Management Industry Code (ACIF C541, 2006); the Billing Industry Code (ACIF V542, 2003), Customer Transfer Industry Code (ACIF C546, 2007); the Complaint Handling Industry Code (ACIF C 547, 2004); and the Consumer Contracts Industry Code (ACIF C620, 2005). The TCP Code and Guidelines should be read in conjunction with the Telecommunications Act 1997 (Cth) and related legislation that includes: the Telecommunications (Consumer Protection and Service Standards) Act 1999 (Cth); the Competition and Consumer Act 2010 (Cth); State and Territory fair trading legislation, where relevant; State and Territory door-to-door sales legislation, the Privacy Act 1988 (Cth); the Spam Act 2003 (Cth); and Do Not Call Register Act 2006 (Cth). This means that the TPC Code is applicable to a number of sectors relating to telecommunications, fair trading, advertising and direct marketing.

50 Telecommunications Act 1997 (Cth) s 109 defines such activities to include: carrying on business as a Carriage Service Provider; and the supplying goods or services for use in connection with the supply of a Listed Carriage Service.

51 See TCP Code cl 1.3.3. It provides that ‘the Code applies only to residential and small business consumers and regulates matters relating to their relationship with their Carriage Service Providers’.
Whilst the Privacy Act exempts some data collectors such as small businesses (see chapter 6 at [6.2.1.1]; [6.2.1.2.]), there is no similar exemption in relation to the TCP code.\footnote{According to the Australian Bureau of Statistics Internet Activity Survey (IAS) there are between 1 001-10 000 medium sized ISPs subscribers as at December 2011. See Australian Bureau of Statistics Website at <http://www.abs.gov.au/ausstats/abs@.nsf/Lookup/8153.0Chapter5Dec%202011>.} The TCP Code also provides that all organisations involved in the telecommunications industry are required to comply with billing, prices, terms and conditions and credit management obligations in the TCP Code, and measures to safeguard personal information of its customers.\footnote{TCP Code cl 6.8 provides that ‘A Supplier must protect the privacy of each Customer’s Billing and related personal information’.} So in contrast to the Privacy Act and NPPs, the TCP Code appears to provide stronger information privacy protection than the NPPs since it covers all those involved in the telecommunications industry including ISPs that are small businesses, and contractors involved in the telecommunications industry.\footnote{Telecommunications Act 1997 (Cth) pt 3 provides that the Act apply to ‘carriers’; and pt 4 provides that the Act applies to ‘service providers’.}

Another advantage under the TCP Code is the provision for Code review after 2 years of the Code being registered by the ACMA and every 5 years subsequently, or earlier in the event of significant developments that impact on the Code or Guideline or a chapter within the Code or Guideline. The TCP Code is currently being reviewed in the context of recent legal and regulatory developments.\footnote{The TCP Code was registered with ACMA on the 19 May 2008 and it is currently being reviewed. See Communications Alliance, ‘Review of Telecommunications Consumer Protection (TCP) Code’ (2007) <http://www.acma.gov.au/webwr/telecomm/industry_codes/codes/c628_2007.pdf> (Last updated 8 August 2011) (Accessed on 02 December 2011).} These developments include: the new provisions of the Australian Consumer Law;\footnote{Australian Consumer Law (‘ACL’) is in Schedule 2 of Competition and Consumer Act 2010 (Cth).} on unfair terms in standard form contract (see chapter 4 at [4.2.2.5]); the amendment to the Telecommunications Act; and the Federal Government’s review of the regulation of the Privacy Act.\footnote{See Communications Alliance Ltd, ‘Review of the Telecommunications Consumer Protection s (TCP) Code’ (2010).} Regular review of the TCP Code\footnote{See Communications Alliance Ltd. Website for details of review of TCP Code at <http://www.commsalliance.com.au/Activities/committees-and-groups/tcpsg> (Accessed on 2 December 2011).} ensures that the industry remains current and adapts rapidly to changes in the telecommunications environment where new products and technologies are introduced which have an impact on the privacy of individuals.\footnote{The Telecommunications Consumer Protection (TCP Code was reviewed by the ACMA in 2007 and early 2008. It was subsequently reviewed in 2010. Refer to Telecommunications Consumer Protection (TCP) Code Review Steering Group (3 August 2011) at<http://www.commsalliance.com.au/Activities/committees-and-groups/tcpsg>.} The ACMA as the code regulator has held a public inquiry
into the complaint handling process in the telecommunications industry. This review suggests that in relation to a small segment of commercial industry, the telecommunications industry, the industry code through its regulator the ACMA, does provide opportunities for a rapid response to a changing technological and legal environment.

The issues of complaints, compliance and enforcement of the TCP Code are discussed in chapter 8.

### 7.5.2 Australian E-Marketing Code of Practice 2005 (‘e-Marketing Code’)

The Australian e-Marketing Code has been developed by the electronic marketing (e-marketing) industry in compliance with the provisions of Telecommunications Act s112 (1A) and the Spam Act. The Australian e-Marketing Code of Practice 2005 (hereafter referred to as the ‘e-Marketing Code’) registered in March 2006, establishes and sets comprehensive industry-wide rules and guidelines for sending commercial electronic messages for e-marketing purposes. The Spam Act does not, however, define e-Marketing nor provide specific guidance to participants in the e-Marketing industry involved in email or mobile marketing on how industry practice should be adapted to ensure compliance with the Spam Act. The provisions of the e-marketing code must comply with legislative requirements set out in the Telecommunications Act and Spam Act. The e-Marketing Code imposes obligations on industry members on the sending of commercial electronic messages in an email or mobile marketing environment to:

---


61 E-marketing is defined under the Telecommunications Act 1997 (Cth) as is: ‘an activity undertaken by an individual or organisation: to market, promote or advertise its own goods and services where sending or causing to send commercial electronic communications is the sole or principle means of marketing, promoting or advertising its own goods and services; that by contract (or other arrangement with) a person markets, advertised or promotes the goods or services (including land and interests in land and business and investment opportunities ) of that person by sending commercial electronic communications or causing them to be sent; that by contract (or other arrangement with) a person markets, advertised or promotes that person as a supplier, prospective supplier, provider or prospective provider of goods or services (including land and interests in land and business and investment opportunities) by sending commercial electronic communications or causing them to be sent.’ Telecommunications Act 1997 (Cth) s 109A.

62 The e-Marketing industry is defined in the Telecommunications Act 1997 (Cth) s 7 as ‘an industry that involves in carrying on an e-marketing activity’.

63 Telecommunications Act 1997 (Cth) s 112 (1) recognises the intention of the Commonwealth Parliament of Australia that industry bodies or associations representing sections of the e-Marketing industry should develop industry codes of practice that are applicable to the sector of the industry involved in e-marketing.

64 See Australian e-Marketing Code of Practice 2005.
• obtain and maintain consent;
• keep records of consent;
• include accurate information about senders/message authorisers;
• provision and operation of a functional unsubscribe facility;
• sending commercial electronic messages about age sensitive material;\(^{65}\)
• complaints handling;\(^{66}\) and
• prohibition of viral marketing campaigns.

It appears that the scope of the e-Marketing Code is wider than the NPPs. Firstly, unlike the NPPs the e-Marketing Code covers all those involved in e-marketing. So that small businesses exempt under the Privacy Act and the NPPs are subject to this code. There are no such exemptions under the Spam Act and the code applies to all those that use personal information individuals, small businesses, media and political parties.

Secondly, in contrast to the Privacy Act NPP 2.1\(^{67}\) the consent provision under the e-Marketing Code requires that industry members must obtain and maintain consent; and to keep records of consent (see chapter 6 at [6.2.2.2.3]. The consent requirement under Spam Act that applies to e-Marketing also sets a higher standard of protection for consumer’s personal information than the NPPs.\(^{68}\) In this area, the impact of legislation, particularly

\(^{65}\) Clause 11 of the e-Marketing Code of Practice (March 2005) relate to sending age-sensitive commercial communications. e-Marketing Code of Practice (March 2005) cl 11.1 provides that ‘where the content of a Commercial Communications seeks to promote or inspire interaction with a product, service or event that is age sensitive, the Message Originator must take reasonable steps to ensure that such content is sent to Recipients who are legally entitled to use or participate in the product service or event, (See Section F, Guideline 10)’. The e-Marketing Code does not define the meaning of ‘age-sensitive commercial communications’ but it could perhaps exclude minors in relation to some material.


\(^{67}\) Privacy Act 1988 (Cth) NPP 2.1 (a) provides that an organisation is not required to obtain express consent to the secondary use of personal information if the secondary purpose is related to the primary purpose of collection and if the personal information is sensitive information, directly related to the primary purpose of collection; and if the individual would reasonably expect the organisation to disclose the information for secondary purposes’.

\(^{68}\) See discussion in chapter 6 [6.2.2.2.3]. Although consent may be inferred from previous or existing relationship or if there is reasonable expectation on the part of the receiver that electronic commercial messages may be sent to the recipient, the Spam Act provides that commercial electronic messages must contain a functional unsubscribe facility (see Spam Act s 18). Non-compliance with the requirement of the Spam Act will give rise to civil remedies, and pecuniary remedies by the courts. The penalties for breach of the Spam Act include fines up to $1.1 million per day, forfeiture of profits from spamming, and compensation to spam victims.
the Spam Act, has led to increasing protection for e-commerce users. Compliance, enforcement and remedies under the e-Marketing Code are examined in chapter 8.

7.6 Conclusion

The Australian regulation and supervision of industry codes is a patchwork of different codes operating under different statutory regulators appointed under specific legislation in the commercial sector. This means that the e-commerce user’s remedies are not necessarily channelled through a single supervisory authority such as the Australian Information Commissioner but rather through a variety of different channels depending on the regulator. For the e-commerce user this is hardly a satisfactory outcome. The e-commerce user is left to try and decide for themselves the appropriate channel for complaint and to determine for themselves which avenue is likely to be more fruitful in terms of outcome. A single supervisory authority which deals with privacy matters will provide a clear line of communication and complaint for the e-commerce user where their privacy has been breached.

Industry codes established under the different legislation, such as the TCP Code and the e-Marketing Code reflect the specific requirements of legislation that set different requirements for compliance. Code requirements may impose greater obligations than the Privacy Act and the NPPs. Firstly the two codes examined have a broader coverage of the types of personal information subject to the Code in contrast to the NPPs: the TCP Code covers aspects of a customers’ billing information such as the customer’s billing name, options, debts and credits outstanding, direct debit information, billing enquires, telephone numbers, and postal addresses, and the e-Marketing Code covers email addresses. Secondly, in contrast to the NPPs that allow secondary use of primary data for direct marketing without express consent of the data subject, the e-Marketing Code and the TCP Code both require express consent prior to the use and/or disclosure of personal information for secondary purposes. A single set of unified privacy principles would provide much needed clarity to the obligations of all parties. Such unified privacy principles can underpin and provided minimum standards for industry codes under all privacy law in Australia.


70 Refer to chapter 4 [4.2], chapter 6 [6.2.3.2] for a detail discussion on the ‘consent’ provision and its effect on information privacy protection for individuals.
In contrast to a Code review (see above at [7.5.1]), a review of the Privacy Act and NPPs appears to be more complex, and the process takes much longer.\footnote{Privacy Act 1988 (Cth) ss 30-33.} The then Office of the Privacy Commissioner undertook a review of the Privacy Act in August 2004, the report was completed in March 2005.\footnote{A subsequent submission was made to the Australian Law Reform Commission’s Review of Privacy in February 2007. See Office of the Privacy Commissioner, Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988 (Cth) (2005); Office of the Privacy Commissioner, Submission to the Australian Law Reform Commission’s Review of Privacy – Issues Paper 31 (February 2007); Office of the Privacy Commissioner, Submission to the Australian Law Reform Commission’s Review of Privacy – Discussion Paper 72 (December 2007); see also Australian Law Reform Commission, above n 15.} Between the years 2004 and 2011, there has been rapid development in technology that has made the provisions of the Privacy Act and NPPs unresponsive to new developments (see chapter 6 at [6.2]) and the required legislative change has been slow to respond. The provision for regular Code review provides significant advantages over the slow and complex requirements of legislative amendment. A review of the Codes allows an industry regulator to systematically and regularly update its monitoring strategy to ensure it reflects the changing regulatory risks and the effectiveness of Code provisions. It also allows regulators to evaluate consumer attitudes and concerns and how codes can be improved to provide effective protection for consumers.\footnote{See generally, Communications Alliance Ltd., “Telecommunications Consumer Protection (TCP) Code Review Steering Group” (3 August 2011) available at <http://www.commsalliance.com.au/Activities/committees-and-groups/tcpsg>.} But the disadvantage of multiple regulators with powers to handle complaints is that there are several multi-layered complaints processes starting with the provider and concluding with an industry established dispute resolution scheme. Chapter 8 explores the issues caused by having different regulators monitoring compliance, handling complaints, enforcing privacy provisions contained in industry codes, and the potential for different sanctions and remedies for an interference with an individual’s information privacy.
Chapter 8: Complaints Handling, Compliance, and Enforcement

8.1 Introduction

Previous chapters examined the protection of privacy in Australia through the federal statutory regime under the Privacy Act NPPs and under approved Industry Codes. This chapter examines the issue of compliance with the NPPs and approved industry codes. It also examines how complaints are handled and the remedies available to e-commerce users for privacy breaches.

The Australian Information Commissioner generally oversees compliance with the NPPs.\footnote{See Privacy Act 1988 (Cth) s 27.} The Australian Information Commissioner’s compliance activities include: providing guidelines for the collection, use and disclosure of personal information, responding to telephone and written enquiries about privacy issues, investigating complaints, resolving individual complaints, and conducting own motion investigations.

This chapter commences by examining how e-commerce users can complain when they believe their privacy has been infringed under the NPPs and Industry privacy Codes. It then turns to the question whether there is evidence of actual compliance with the Privacy Act NPPs and industry codes. It concludes with an examination of civil enforcement, remedies and sanctions for breach of individual privacy.\footnote{All statistical information referred to in this chapter has been compiled from the Annual Reports, and submissions made to regulatory bodies such as the then Office of the Privacy Commissioner (now the Office of the Australian Information Commissioner), Australian Law Reform Commission, New South Wales Law Reform Commission, Australian Media and Communications Authority, and the Telecommunications Industry Ombudsman. Details are provided in the Tables below.}

8.2 Complaints

in relation to complaints handling and investigation; and thirdly, the outcomes of
complaints investigated by the Australian Information Commissioner, the ACMA
[telecommunications], and the TIO [telecommunications ombudsman].
This is discussed first in relation to the Privacy Act and then in relation to telecommunications.

1.4.1 Privacy Act

A complaints process for breach of the NPPs is set out in Privacy Act pt V. It is a key
function of the Australian Information Commissioner to receive and handle complaints.
The Australian Information Commissioner is the only avenue for complaint for breach of
NPPs. The Australian Information Commissioner’s power to investigate breach of NPPs
is set out in the Privacy Act s 27 (1). The Commissioner will only investigate and
determine complaints in relation to breaches of the NPPs and approved privacy codes
after a complaint has been lodged. If a written complaint is lodged for breach of the NPPs
or an industry privacy code, the complaint may be investigated under Privacy Act s 36.
The Commissioner may also investigate and undertake on its own motion investigations
if there may be an interference with privacy. Investigations are discretionary.

For details on outcomes of complaints investigated by the Office of the Australian Information
Commissioner, TIO, and ACMA refer be to Tables 8.8-8.10 below.

Privacy Act 1988 (Cth) pt V provides for investigation, ss 36–53B provide for lodging a complaint for
breach of the Privacy Act and powers of determination of the Australian Information Commissioner.
Section 36(1A) of the Act there is no right to complain to the
Australian Information Commissioner about acts and practices of an organisation that is bound by an
approved privacy code where the code provides for a procedure for making dealings with complaints to an
adjudicator

Privacy Act 1988 (Cth) pt III allows nonexempt organisations to apply to the Australian Information
Commissioner for approval of a privacy code that replace the NPPs. Refer to the discussion in chapter 7 at
[7.3].

Privacy Act 1988 (Cth) s 40(2) provides for ‘own motion investigation’ investigation by the Privacy
Commissioner into an act or practice without a complaint having been made. Cases investigated under the
own motion investigation powers by the Privacy Commissioner include: Own Motion Investigation v
Telecommunications Company [2010] PrivCmrA 16; Own Motion Investigation v Information Technology

Privacy Act 1988 (Cth) s 36 provides for an individual to make a complaint if an act or practice is an
interference with the individual’s privacy; s 38A provides that the Privacy Commissioner has a discretion not
to continue as a representative complaint or decide not to investigate, or may defer investigation if he or she
finds that the act or practice is not an interference under the circumstances under s 41; or under 40(1B) where
the act or practice is not an interference with privacy; the complaint is frivolous, vexatious, misconceived or
lacking in substance or the act or practice is subject to the law; if the complainant has complained to the
respondent and the respondent has adequately dealt with the complaint, or not had adequate opportunity to
deal with the complaint. All reference to the Privacy Commissioner is to be read as the Australian
Information Commissioner as the Privacy Commissioner is now known as the Australian Information
Commissioner.
and the consequences for those individuals, the sensitivity of the personal information involved, the progress of an agency’s or organisation’s own investigation into the issue, and the likelihood that the investigation will reveal acts or practices that involve systemic interferences with privacy and/or that are unidentified, widespread or on going.  

There are two ways the Australian Information Commissioner can resolve a complaint after investigation. The first is resolving through conciliation to effect a settlement between the complainant and the respondent; and the second is by making a determination either to dismiss the complaint or find the complaint substantiated. A determination is made following investigation of the complaint under Privacy Act s 52. The Office of the Privacy Commissioner’s Annual Report for the years 2006-2011 has not reported a single determination made by the Privacy Commissioner. Consequently, conciliation in that period was the sole method of dispute resolution.

As noted earlier in chapter 7 at [7.3], there are just a handful of approved codes under the Privacy Act so essentially in relation to sectors other than the telecommunications industry, the Commissioner’s role in handling complaints is especially important. But in relation to approved privacy codes in sector specific industry codes such as the TPC Code and the E-marketing Industry Code that are regulated under the provisions of the
Telecommunications Act and the Spam Act respectively, although the Commissioner is consulted as to whether it complies with the requirements of the Privacy Act NPPs, the Commissioner has no authority to receive complaints directly for breach of such Codes.\textsuperscript{89} This is because there are separate industry based-complaint handling processes. The TCP Code and the E-marketing Industry Code each has its own code adjudicator and privacy complaints related to the communications sector are dealt with under that code.\textsuperscript{90}

Diagram 8.1 below gives an overview of the process of complaints handling, investigation, and resolution under the Privacy Act for breach of the NPPs (s 27(1) (ab)).

\textsuperscript{89} See Privacy Act 1988 (Cth) s 36(1A) (a)-(b).

\textsuperscript{90} Refer to chapter 7 at [7.6]. For example complaints may be made about spam emails to ACMA and not to the Australian Information Commissioner. See Telecommunications Act 1997 s 112 which provides that organisations and associations involved in the telecommunications industry may develop industry codes. Such industry codes must satisfy the criteria set under the Act before it will be registered by ACMA. Note that this only applies to Privacy Act approved codes and not codes under the Telecommunications Act 1997.
Diagram 8.1: Investigation and Resolution Process for Breach of NPPs

Breach of NPPs (Privacy Act s 36)

- No investigation if complaint is not lodged with respondent first (Privacy Act s 40(1A))
- Complaint to the Respondent (Privacy Act s 40)
  - Conciliation process begins (Privacy Act ss 27 (1) (a), 27 (1) (ab))
  - If resolved through conciliation - No action
    - If conciliation unsuccessful
      - Preliminary inquiries (Privacy Act s 42)
      - Privacy Commissioner investigates (Privacy Act ss 40, 43)
        - Attend compulsory conference (Privacy Act ss 46, 47)
          - Failure to attend compulsory conference without lawful excuse:
            - If individual - maximum fine of $1,000; and/or maximum 6 months imprisonment or both; or
            - If body corporate – maximum fine of $5,000 maximum. (Privacy Act s 46)
            - Determination to dismiss or declares:
              - that respondent not repeat or continue such conduct; or
              - complainant entitled to compensation or damages; or
              - no further action (Privacy Act s 52(1)).

(Source: Diagram 8.1- Created by author).
The next section examines problems for effective privacy complaints handling under the Privacy Act.

8.2.1.1 Privacy Act: Complaints Effectiveness

It is to be noted that the Information Commissioner’s role in relation to complaints is to provide the last rather than the first level of recourse. There are a number of hurdles before the Commissioner accepts and investigates a complaint, firstly the complaints must be in writing (if not then it will be noted as an inquiry); secondly complainants must contact the respondent in the first instance; thirdly the respondent must be given reasonable time to respond.

First, the ratio of telephone inquiries and written inquiries to written complaints is significant, as indicated in the Tables 8.1 and 8.2 set out below. So even if there are telephone and written enquires these enquires may not amount to a complaint nor give a right to redress and remedy.

Secondly, a complainant can only resort to the Commissioner after failure to resolve the complaint with the organisation. The failure to do so is a common reason for dismissal of complaints by the Commissioner as is the requirement that the organisation have sufficient time to resolve the complaint. Another common ground for refusal is that there is no interference with privacy. So that even if an e-commerce user went to the effort of filing a written complaint, the chances of an investigation and outcome are quite small as is evident from Tables 8.1, 8.2, 8.3, and 8.8 set out below. So, for example Table 8.3 below indicates that in the period 2008-11, over 50% of written complaints were closed without investigation. Between the years 2008-11, 26 complaints were closed without investigation on the ground that the complainant had failed to raise the complaint with the provider first. There is trade-off between efficiency on the one hand which ensures that only those who have a serious complaint will take the effort to lodge a written complaint; and on the other hand using inquiries to provide information about potential problems and

---

91 The Office of the Australian Information Commissioner in its Annual Report 2010-11 reports that telephone and written enquiries to the Australian Information Commissioner’s office range of about 20 000 per year. See Table 8.1 below.
92 Privacy Act 1988 (Cth) s 41(1) (a).
93 Privacy Act 1988 (Cth) s 41(2) (b).
94 Privacy Act 1988 (Cth) s 41(1) (a).
95 See Table 8.3 NPP and Non NPP written complaints closed without investigation by OPC for 2008-10, and AOIC for 2010-11.
possible remedies. This because the Commissioner may close complaints if he/she is of the opinion that there is no breach or following conciliation that the matter has been adequately dealt with. Minor complaints not involving serious harm are very unlikely to be investigated.  

Despite this low complaint to inquiry ratio, the ALRC has recommended that the Australian Information Commissioner be given additional powers to refuse to investigate complaints in certain circumstances for example, if the complaints are frivolous, vexatious, misconceived, or lacking in substance or have no prospect of achieving a practical or satisfactory resolution. This recommendation suggests that many complaints are trivial or lack substance. This, however, flies in the face of growing evidence of wholesale breach of e-commerce user’s private information and increasing concern about privacy issues by consumers. It is, of course, possible that the Commissioner receives high volumes of trivial complaints with the more serious complaints not being brought to the Commissioner at all. If this is the case, it may be that e-commerce users are unaware that they have recourse against organisations that breach privacy obligations. Alternative explanations are that e-commerce users are unaware of serious breaches or have given up on obtaining a remedy. Any of these alternatives suggest serious difficulties in achieving protection for the e-commerce user. Of course it might be that the e-commerce user has suffered no significant loss or damage, or that that organisations are compliant or resolve most disputes before they come to the Commissioner. But if there is little investigation or monitoring, it is impossible to know whether there is compliance (see below at [8.3.1]; [8.3.1.1]). Formal complaints, most likely do not represent the level of privacy breach.

98 See Table 8.3 below. See Australian Law Reform Commission, above n 97 [49.10].
99 Refer to chapter 2 at [2.2.2]. According to surveys on attitudes towards data protection conducted by the European Union, 74% of Europeans see that disclosing persona information as unavoidable in an increasing part of modern life however 72% of internet users worry that they are giving away too much personal information and that they have no control of their personal information. As a result users’ lack of trust in online transactions and services has held back the growth of digital economy. See European Commission Justice, ‘Why Do We Need an EU Data Protection Reform?’ European Union, Justice, JusticeNewsroom, (online) June 2011 (Date accessed 26/07/2012) <http://ec.europa.eu/justice/newsroom/data-protection/news/>.
100 Australian Communications Consumer Action Network (ACCAN), ‘Research reveals telco complaints are under reported’ (23 November 2010).
Most dissatisfied consumers never complain. According to Hyman et al., only a portion of the problems/defects that exist are actually perceived; only a portion of these perceived are voiced; only a portion of those voiced gain access to a complaint-resolving party; and only a portion at each stage are resolved successfully. Hyman suggests that as many as 54 per cent of consumers complain to someone else. Similarly, the technical Assistance Research Program (TARP) in the U.S suggests that as many as 95% of dissatisfied customers do not complain to the company concerned. Research commissioned by the Australian Communications Consumer Action Network (ACCAN) found that only 7% of those who are dissatisfied with the way their telecommunications service provider has handled a problem or complaint take it to the Telecommunications Industry Ombudsman. This at least, suggests that the same might be true in relation to those complaints within the jurisdiction of the Australian Information Commissioner. In relation to the Australian telecommunications industry instead of complaining most consumers will opt to change providers. One such case relate to the case of the Telstra’s mail-out bungle in 2010 which resulted in a breach of privacy. Telstra had mailed out some 220,000 customers personal information and telephone plans including 23,500 silent-line customers. Whilst it might be said that the ‘market’ is working to provide people with a choice whether to use a provider that conforms with privacy protection regulation rather than to stay with a provider that does not conform with privacy regulation, this assumes rational consumers acting in their own best interests. There is no information whether this trend also applies in relation to those e-commerce providers bound by the NPPs.

For these reasons the statistics on complaints cannot be taken to be as an indicator that there is a high level of compliance with the NPPs (see Table 8.2 below). What might be more useful is the number of inquiries made by individuals rather than the number of complaints formally lodged with the Australian Information Commissioner.

---

102 Ibid; see also the Office of the Privacy Commissioner, above n 96, 147.
103 Drew Hyman et al, above n 101.
105 See study commissioned by Australian Communications Consumer Action Network (ACCAN), Privacy Complaints: In search of the Right Path’ and undertaken by Cyberspace Law and Policy Centre, University of New South Wales, (2010).
Tables 8.1 and 8.2 below show the ratio of inquiries to finalised complaints. Table 8.3 below relate to the ratio of NPP related and non NPP related complaints that are closed without investigation by the Office of the then Privacy Commissioner and the current Australian Information Commissioner.

### Table 8.1: Telephone and Written Enquiries Received by the OPC for 2008-10 and the OAIC for 2010-11

<table>
<thead>
<tr>
<th>Reporting Years (1 July-30 June)</th>
<th>Total Telephone enquiries</th>
<th>Written enquiries (via e-mails, letters, and fax)</th>
<th>Total telephone &amp; written enquiries</th>
<th>Total % of NPP related enquiries</th>
</tr>
</thead>
<tbody>
<tr>
<td>2008-2009 (NPP related)</td>
<td>21 178 (9 447)</td>
<td>2 078 (1 350)</td>
<td>23 356 (10 798)</td>
<td>46.23%</td>
</tr>
<tr>
<td>2009-2010 (NPP related)</td>
<td>20 935 (9 510)</td>
<td>1 909 (1 432)</td>
<td>22 844 (10 942)</td>
<td>47.90%</td>
</tr>
<tr>
<td>2010-2011 (NPP related)</td>
<td>20 617 (10 986)</td>
<td>1 909 (1 721)</td>
<td>22 526 (12 713)</td>
<td>56.44%</td>
</tr>
<tr>
<td>TOTAL (NPP related)</td>
<td>62 730 (29 943)</td>
<td>4 986 (4 503)</td>
<td>68 726 (34 453)</td>
<td>50.13%</td>
</tr>
</tbody>
</table>

(Source: Table 8.1 - Created by author).<sup>107</sup>

### Table 8.2: Written complaints and Own Motion Investigations (OMIs) closed by the OPC for 2008-10 and the OAIC for 2008-11

<table>
<thead>
<tr>
<th>Reporting Year (1 July-30 June)</th>
<th>Total written (IPPs &amp; NPPs related) complaints</th>
<th>Written complaints (NPP related)</th>
<th>Own Motion Investigations (including Data Breach Notification (“DBN”))</th>
<th>Total Complaints handled (written &amp; OMIs)</th>
<th>Total (written &amp; OMIs) complaints closed</th>
</tr>
</thead>
<tbody>
<tr>
<td>2008-2009</td>
<td>1 089</td>
<td>635</td>
<td>83 (10)</td>
<td>1 172</td>
<td>1 357</td>
</tr>
<tr>
<td>2009-2010</td>
<td>1 201</td>
<td>639</td>
<td>117 (44)</td>
<td>1 318</td>
<td>1 203</td>
</tr>
<tr>
<td>2010-2011</td>
<td>1 222</td>
<td>703</td>
<td>99 (56)</td>
<td>1 321</td>
<td>1 167</td>
</tr>
<tr>
<td>Total</td>
<td>3 512</td>
<td>1 977</td>
<td>299 (110)</td>
<td>3 907</td>
<td>3 727</td>
</tr>
</tbody>
</table>

(Source: Table 8.2 - Created by author).<sup>108</sup>

---


<sup>108</sup> All statistics on written complaint and Own Motion Investigations has been compiled by the by the Office Privacy Commissioner and the Office of the Australian Information Commissioner is extracted from the
Table 8.3: NPP and non NPP related complaints closed without investigation by the OPC for 2008-10 and the OAIC for 2010-11

<table>
<thead>
<tr>
<th>Reporting Year (1 July - 30 June)</th>
<th>2008 - 2009</th>
<th>2009 - 2010</th>
<th>2010 - 2011</th>
<th>2008 - 2011</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total written complaints received</td>
<td>1089</td>
<td>1201</td>
<td>1222</td>
<td>3512</td>
</tr>
<tr>
<td>Complaints closed without investigation</td>
<td>NPPs</td>
<td>Non NPPs</td>
<td>NPPs</td>
<td>Non NPPs</td>
</tr>
<tr>
<td>No Interference with privacy ( s 41 (1) (a) )</td>
<td>95</td>
<td>73</td>
<td>41</td>
<td>46</td>
</tr>
<tr>
<td>Respondent has adequately dealt with the complaint – s 41 (2) (a)</td>
<td>114</td>
<td>49</td>
<td>47</td>
<td>33</td>
</tr>
<tr>
<td>Respondent has not had an opportunity to deal with complaint – s 41 (2) (b)</td>
<td>3</td>
<td>4</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>Other (e.g. complaint withdrawn or being dealt with under another law)</td>
<td>32</td>
<td>24</td>
<td>19</td>
<td>16</td>
</tr>
<tr>
<td>Total</td>
<td>244</td>
<td>150</td>
<td>109</td>
<td>99</td>
</tr>
<tr>
<td>Total for year</td>
<td>394</td>
<td>208</td>
<td>159</td>
<td>762</td>
</tr>
</tbody>
</table>

(Source: Table 8.3 - Created by author).

It is remarkable that of the total telephone and other inquiries for the years 2008-09, (10,798), 2009-10 (10,942) and 2010-11 (12713) (see Table 8.1 above), but only 635, 639 and 703 (see Table 2 above) respectively resulted in written complaints that were NPP related. Some of the reasons for this low written complaints rate have been mentioned above.

One of the factors which may influence lodgement of complaints is the delay in resolution. The average time taken to resolve a complaint by the Commissioner depends on how


complex the matters are to resolve.\(^{110}\) The Australian Information Commissioner aims to resolve all complaints in an average of four months. The time frame for resolving less complicated complaints is a few weeks and for more complex complaints about 12 months.\(^{111}\) These time frames contrasts with the much speedier resolution of complaints by the ACMA and the TIO (see below at [8.2.2.1]). The issue may be one of resources available to handle complaints as well as lack of clear time lines for complaints handling such as exist with the ACMA and the TIO.

If complaints to the Australian Information Commissioners are not closed within the year they are carried forward to the following year. This means that businesses are under no pressure to comply with privacy laws or required to respond to complaints quickly. There are neither incentives nor sanctions for slow responses. There are also no financial incentives for organisations to resolve complaints themselves rather than allow them to escalate to the Office of the Australian Information Commissioner as the Commissioner does not impose a charge on any party for dispute resolution. One proposal is to give complainants the right to ask for a determination. This would give complainants significant leverage to force respondents to respond to the complaint quickly and where appropriate agree to compensation to avoid the ‘time-consuming’ formal determination process.\(^{112}\) This may be a better option that to legislate a time frame for completing investigations or for resolving written privacy complaints that are lodged with the Commissioner’s office. The ALRC has recommended that the Commissioner be given power in a determination to direct the respondent to take specific action within a specific period for the purpose of ensuring compliance with the Privacy Act.\(^{113}\) This will give organisations greater certainty on what behaviour is consistent with the NPPs or regulation.

As noted above very few inquiries result in formal written complaints. Inquiries, however, provide a valuable resource to identify possible problems and systemic risks that threaten e-commerce user’s privacy. Unlike the TIO, who has the power to investigate systemic risks (see below at [8.3.2.1), the then Privacy Commissioner (now the Australian Information Commissioner) has no mandate to investigate or deal with systemic risks. This

---


\(^{111}\) See Office of the Information Commissioner, Annual Report 1 July 2010-30 June 2011 (2011) 32. The time taken by the former Privacy Commissioner was 2-12 months. See Office of the Privacy Commissioner, above n 107, 53; Cyberspace Law and Policy Centre, above n 87.

\(^{112}\) See Australian Law Reform Commission, above n 97, Submission PR 536, [49.56].

\(^{113}\) Australian Law Reform Commission, above n 97, [49.70].
hampers a thorough investigation of systemic risks. This is highlighted in cases involving Vodafone and Telstra in which the TIO and the ACMA played a pivotal role in investigating systemic risks, as will be discussed below in [8.3.2.1]. Moreover it is telling that the former Privacy Commissioner has not made any formal determinations against any private sector organisation since 2005.\(^{114}\) This contrasts with the much more proactive approach in the telecommunications sector referred to below in [8.3.2.1]. As a consequence of this, opportunities for detection of breaches and providing remedies before serious harm is caused may be lost.

The ALRC has recognised the need for the Commissioner to prescribe remedies that address systemic issues, but also commented that there needs to be a compromise between the need to address individual complaints and addressing systemic issues.\(^{115}\) One view is that the privacy protection fails on both accounts; it neither provides effective privacy protection to the individual e-commerce user nor has the Commissioner has the power or the facilities to address systemic risk issues. It will take political commitment to improve privacy protection and to honour Australia’s human rights obligations. The protection under the Privacy Act and the NPPs will only be effective if the Office of the Australian Information Commissioner is given sufficient resources.\(^{116}\)

Consequently a breach of privacy involving an e-commerce user does not necessarily give rise to a remedy even if the user is aware of the privacy breach and lodges a complaint. It is unlikely in situations where there is online tracking and monitoring, and where personal information is collected without the consent or knowledge of a data subject so that the data subject is not aware of how personal information is being used, for what purpose and by whom. As will be seen in the Table 8.4 following, the most frequent inquiries relate to the collection and use and disclosure of personal information by private sector organisations.

\(^{114}\) Office of the Privacy Commissioner, above n 96, 102; Australian Law Reform Commission, above n 97, [49.10]. The ALRC refers a ‘systemic issue’ as being ‘an organisation’s or industry’s practice rather than about an isolated incident’ and one that can be distinguished from issues that have no implications beyond the immediate actions and rights of the parties to the complaint.

\(^{115}\) Australian Law Reform Commission, above n 97, Submission PR 536, [49.6]-[49.13].

\(^{116}\) Ibid, [49.11].
Table 8.4: NPP related telephone enquiries received by the OPC from 2008-10, and the OAIC from 2010-11

<table>
<thead>
<tr>
<th>Reporting Year (1 July–30 June)</th>
<th>2008-2009</th>
<th>2009-2010</th>
<th>2010-2011</th>
</tr>
</thead>
<tbody>
<tr>
<td>NPP1 - Collection</td>
<td>1 363</td>
<td>1 427</td>
<td>1 581</td>
</tr>
<tr>
<td>NPP2 - Use and Disclosure</td>
<td>2 536</td>
<td>2 670</td>
<td>2 780</td>
</tr>
<tr>
<td>NPP3 - Data Quality</td>
<td>236</td>
<td>268</td>
<td>236</td>
</tr>
<tr>
<td>NPP4 - Data Security</td>
<td>768</td>
<td>732</td>
<td>787</td>
</tr>
<tr>
<td>NPP5 - Openness (Privacy Policy Statements)</td>
<td>159</td>
<td>130</td>
<td>85</td>
</tr>
<tr>
<td>NPP6 - Access and Correction</td>
<td>1 206</td>
<td>1 301</td>
<td>1 164</td>
</tr>
<tr>
<td>NPP7 - Identifiers</td>
<td>17</td>
<td>8</td>
<td>6</td>
</tr>
<tr>
<td>NPP8 - Anonymity</td>
<td>6</td>
<td>10</td>
<td>25</td>
</tr>
<tr>
<td>NPP9 - Transborder Data Flows</td>
<td>50</td>
<td>35</td>
<td>53</td>
</tr>
<tr>
<td>NPP10 - Sensitive Information</td>
<td>114</td>
<td>135</td>
<td>65</td>
</tr>
<tr>
<td>NPP - Exemptions</td>
<td>1 806</td>
<td>162</td>
<td>1 685</td>
</tr>
<tr>
<td>Private Sector Provisions (General)</td>
<td>1 186</td>
<td>1 102</td>
<td>301</td>
</tr>
<tr>
<td>SUB TOTAL</td>
<td>9 447</td>
<td>9 510</td>
<td>8 768</td>
</tr>
<tr>
<td>Non Private Sector Provision Issues</td>
<td>6 147</td>
<td>4 577</td>
<td>2 218</td>
</tr>
<tr>
<td>Issues Unrelated to Privacy</td>
<td>5 854</td>
<td>6 848</td>
<td>9 631</td>
</tr>
<tr>
<td>TOTAL</td>
<td>21 178</td>
<td>20 935</td>
<td>20 617</td>
</tr>
</tbody>
</table>

(Source: Table 8.4 - Created by author).\textsuperscript{117}

The Telecommunications Act imposes obligations on providers concerning the disclosure and use of information gathered in the course of conducting their business. The next section examines how complaints are handled under Telecommunications codes, the TCP Code and the e-Marketing Code.

### 8.2.2 Complaints handling under TCP Code and the e-Marketing Code

The TCP Code and the e-Marketing Code provide complaints handling mechanisms. Under the TCP Code, cl 9.1.8 of the Code requires carriage service providers to identify, record, and resolve complaints. Clause 9.2.5 provides that complaints should be resolved on first contact where possible and that complaints must be finalised within 30 days or as

\textsuperscript{117} All statistics in Table 8.3 has been compiled by the author from the Office of the Privacy Commissioner, ‘The Operation of the Privacy Act Annual Report’ 1 July 2008- 30 June 2009 (2009); Office of the Privacy Commissioner, above n 107; The Office of the Australian Information Commissioner, Annual Report 1 July 2010-June 30 2011 (2011).
soon as practicable in all the circumstances.\textsuperscript{118} This is an important obligation as it enables individual consumers to have their grievances assessed independently, settled quickly, and with no direct cost. Under the TCP Code cl 9.1.8(B), the code authority, that is the ACMA, is required to identify recurring or systemic problems and suppliers must classify and analyse complaints at least every 3 months. This is in contrast to the Privacy Act which does not provide a time frame for complaints to be resolved as previously discussed above at [8.2.1.1], nor impose obligations in relation to systemic risks (see below at [8.2.2.1]).

Besides the ACMA, the Telecommunications Industry Ombudsman (TIO) can also investigate complaints against telecommunications companies (such as ISPs and telecommunications carriers) for breach of the Telecommunications Act. The TIO publishes in its Annual Report information about complaints handling. The TIO categorises complaints into 4 levels. Level 1 is new complaints. Level 2 are cases that are not resolved by referral to the service provider and require the TIO to conciliate. Level three involves cases that require further investigation and in these circumstances the TIO provides advice about outcome. The TIO has the power to make binding decisions at Level 3 if the value of the dispute is below $1200. Level 4, relates to cases that require thorough and detailed investigation where the TIO may make a binding decision or direction.\textsuperscript{119} The TIO can issue a binding determination up to the value of $30,000 if a complaint is not resolved through the TIO process of referral, conciliation or investigation. The TIO’s decision is binding on service providers.\textsuperscript{120} The TIO can also investigate complaints that affect a large number of consumers as a result of systemic issues such as where there is a failure in the systems or processes of a service provider, and recommend potential solutions and seek undertakings from service providers to demonstrate that the service provider has resolved the systemic issues.\textsuperscript{121}

Complaint handling under the e-Marketing Code is provided under cl 12. Under cl 12 a complaint handling system must be fair, confidential and easy to use; records of complaints must be maintained and where requested by the ACMA a summary of

\textsuperscript{118} Code states that: “Where possible, Suppliers must seek to resolve a Complaint on first contact. Complaints must be finalised within 30 days or as soon as practicable in all the circumstances”. In June 2011, ACMA issued 35 notices to various service providers. The responses from service providers indicated that 14 providers resolved more than 80 per cent of complaints on first contact. See ACMA, Telecommunications Consumer Protection, Compliance and Enforcement Bulletin, Issue 6, (September 2011).


\textsuperscript{120} Ibid, 13.

\textsuperscript{121} Ibid, 11.
information received under cl 12.7 must be submitted to the ACMA. In the first instance any complaint about a breach of the Code is handled by the e-marketing company to which the complaint relates that is the company that sent the commercial electronic message or authorised it to be sent. Prior to submitting a complaint to the ACMA, complainants can access the ACMA’s Web site and view the ACMA’s privacy statement, a spam complaints handling policy, and the complaints handling process.

The common elements of the complaints process for a breach of the Spam Act and/or the Do Not Call Register Act provided by the ACMA are that complaints:

- must be in writing (emails are acceptable for spam, and Do Not Call Register complaints),
- may be made to the organisation involved but it is not essential that complainants must proceed with this step first.

The other common element is that there is a right of appeal and review if complainants are dissatisfied with the outcome of the complaint. The complaints received and the outcomes depend on the categories of complaints. The outcome of the complaint is reviewable by the Commonwealth Ombudsman. The two important features of these codes which are not replicated in the Privacy Act are: speedy resolution processes and the provision for regular monitoring by the regulator of the complaints processes and avenues for appeal.

The next section examines the problems for effective privacy complaints handling under industry codes.

8.2.2.1 TCP Code and the e-Marketing Code – Complaints Effectiveness

As the regulator and Code administrator of the TCP Code and the e-Marketing Code, the ACMA regularly receives a large volume of complaints from the communications sector. The ACMA publishes annually separate complaints handling policies for general complaints, spam complaints under the Spam Act, and for complaints received under Do

---


123 For example statistics compiled by Australian Communications and Consumer Action Network provide that ACMA receives 4,000 privacy complaints annually under the Spam Act 2003 (Cth) and about 12,000 privacy complaints per year related to the Do Not Call Register Act 2006 (Cth). See Cyberspace Law and Policy Centre, above n 87.
Complaints about communications privacy issues under industry Codes relate to the inappropriate collection and disclosure of personal information without consent, spam, and misuse of silent telephone numbers registered under the Do Not Call Register. In relation to privacy related complaints, Tables 8.5 and 8.6 following indicates the level of complaints received (Table 8.5) and investigated (Table 8.6) by the TIO for the period 2008-11 relating to privacy.


125 ‘Vodafone denies client data on internet was open to all’ The Australian, (Online, 10 January 2011) <http://www.theaustralian.com.au/australian.../vodafone-denies-client-data-on-internet-was-open-to-all/story-fn4iyzsr-1225984888256>.

### Table 8.5: Privacy Complaints Received by the TIO for 2008-11

<table>
<thead>
<tr>
<th>Reporting Year (1 July-30 June)</th>
<th>2008-2009</th>
<th>2009-2010</th>
<th>2010-2011</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Privacy Complaints Received</td>
<td>175,946</td>
<td>167,772</td>
<td>197,682</td>
</tr>
<tr>
<td>A. Breakdown of privacy related complaints</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Life threatening calls and communications</td>
<td>39</td>
<td>26</td>
<td>38</td>
</tr>
<tr>
<td>Unwelcome calls/communications (such as menacing, offensive or harassing calls/communications)</td>
<td>762</td>
<td>792</td>
<td>676</td>
</tr>
<tr>
<td>Telecommunications service provider telemarketing or sending MPS marketing messages to consumer even after being asked to stop</td>
<td>433</td>
<td>441</td>
<td>355</td>
</tr>
<tr>
<td>Access to information denied, or inaccurate information held by provider</td>
<td>1,529</td>
<td>2,057</td>
<td>1,893</td>
</tr>
<tr>
<td>Manner of information collected, stored or disposed contrary to Australian privacy law</td>
<td>198</td>
<td>220</td>
<td>214</td>
</tr>
<tr>
<td>Inadequate advice about preventing spam to consumers</td>
<td>19</td>
<td>23</td>
<td>24</td>
</tr>
<tr>
<td>MPS content supplier’s failure to warn a consumer about the danger of disclosing personal information via chat services New issue keyword introduced 1 July 2009</td>
<td>N/A</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>Spam from a telecommunications service provider</td>
<td>19</td>
<td>28</td>
<td>32</td>
</tr>
<tr>
<td>Disclosure of a consumer’s silent telephone number</td>
<td>241</td>
<td>216</td>
<td>228</td>
</tr>
<tr>
<td>Consumer’s personal information relating to account disclosed, (silent telephone number not included)</td>
<td>618</td>
<td>465</td>
<td>787</td>
</tr>
<tr>
<td>Total</td>
<td>3,858</td>
<td>4,271</td>
<td>4,248</td>
</tr>
</tbody>
</table>

(Source: Table 8.5- Created by author).  

It is clear from the above table that there are significant levels of complaints relating to individual privacy. But quite a small proportion of these complaints result in formal investigations. For example of the 198 complaints relating to the manner of information,  

---

collected, stored or disposed of contrary to privacy law, only 17 were investigated. It is not clear why this might be so. It may be that when the complaint is lodged the organisation has greater incentive to resolve the complaint or that the complaint has no foundation, is trivial or the complainant simply gives up. As previously discussed above in [8.2.2], there are 4 levels of investigation undertaken by the TIO. The majority of complaints do not reach level 4 complaints. An escalation of complaints to level 4 becomes expensive for a member organisation. TIO encourages early resolution of complaints as if it reaches level 4 it can be expensive for members who bear the costs.

**Table 8.6: Privacy Complaints Investigated by the TIO for 2008-11**

<table>
<thead>
<tr>
<th>Privacy complaint</th>
<th>2008-2009</th>
<th>2009-2010</th>
<th>2010-2011</th>
</tr>
</thead>
<tbody>
<tr>
<td>A provider not following correct procedure for dealing with life threatening communications</td>
<td>2</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>A provider not following correct procedure for dealing with unwelcome communications</td>
<td>54</td>
<td>65</td>
<td>52</td>
</tr>
<tr>
<td>A telecommunications provider has continued telemarketing the consumer or sending MPS marketing messages after being asked to stop</td>
<td>27</td>
<td>30</td>
<td>21</td>
</tr>
<tr>
<td>Access to information being denied, or information held by the provider being inaccurate</td>
<td>239</td>
<td>406</td>
<td>283</td>
</tr>
<tr>
<td>Complaint about information being collected, stored or disposed in a manner that is contrary to Australian privacy law</td>
<td>17</td>
<td>29</td>
<td>23</td>
</tr>
<tr>
<td>Failure of a telecommunications provider to give adequate advice or assistance to a consumer in relation to spam prevention</td>
<td>4</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>Spam received from a telecommunications service provider</td>
<td>3</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>Disclosure of a consumer’s silent telephone number</td>
<td>60</td>
<td>50</td>
<td>50</td>
</tr>
<tr>
<td>Disclosure of personal information relating to a consumer’s account, other than the disclosure of a silent telephone number</td>
<td>117</td>
<td>111</td>
<td>102</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>523</strong></td>
<td><strong>698</strong></td>
<td><strong>537</strong></td>
</tr>
</tbody>
</table>

(Source: Table 8.6 - Created by author).\(^{128}\)

Of the total privacy related complaints received by the TIO for the years 2008-09 (3858), 2009-10 (4271) and 2010-11 (4248), only 523, 698, and 537 respectively resulted in an

investigation by the TIO. Some of the reasons for this low rate of investigation have been mentioned above. The ACMA is the relevant regulator who deals with complaints under the Do Not Call Register Act and the Spam Act. The number of complaints relating to direct marketing and Spam are set out in the Table 8.7 below.

Table 8.7: Complaints Opened and Closed under the Do Not Call Register Act 2006 (Cth) and Spam Act 2003 (Cth) by ACMA for 2008-11

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>DNCR 129</td>
<td>12 057</td>
<td>11 229</td>
<td>16 036</td>
<td>39 322</td>
</tr>
<tr>
<td>Telemarketing &amp; Fax- marketing 130</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Spam</td>
<td>3 947</td>
<td>3 017</td>
<td>2 571</td>
<td>9 535</td>
</tr>
<tr>
<td>Total</td>
<td>16 004</td>
<td>14 246</td>
<td>18 607</td>
<td>48 757</td>
</tr>
</tbody>
</table>

(Source: Table 8.7: Created by author). 131

The timelines imposed on telecommunication industries generally result in speedy resolution of complaints. The volume of privacy complaints 132 to the ACMA (industry regulator) and the TIO (industry dispute resolution scheme ombudsman, i.e. TIO Scheme) are higher than that received by the then Office of the Privacy Commissioner in relation to the same time periods. 133 Complaints to the TIO 134 are approximately 260,000 per year of which about 5,000 relate to privacy issues. The TIO resolves 90% of complaints within 10 days and 3-4 months for more complex issues. 135 The ACMA, the industry regulator, takes an average of 2-5 days for simple complaints and about 3-4 months for complex matters. 136 This compares more favourably with the average time taken for privacy complaints dealt

---

129 Do Not Call Register (“DNCR”).
131 The statistics in Table 8.7 has been compiled by the author from statistics provided in the ACMA’s Annual Report 2008 -11.
132 Office of the Privacy Commissioner, above n 96, 132, 146; Refer also to chapter 7, Table 7.1 for statistics on breach of ADMA Code for the period 1999–2010 to make a comparison of the level of complaints to industry regulators with that made to the Privacy Commissioner in Table 8.3.
134 For more information refer to the Telecommunications Industry Ombudsman (TIO), ‘Annual Report 2009’; see also A Cyberspace Law and Policy Centre, above n 87.
135 Ibid.
136 Australian Communications and Media Authority, above n 107, 95.
with by the then Office of the Privacy Commissioner (now Office of the Australian Information Commissioner) (see above at [8.2.1]; [8.2.1.1]). It is apparent from the above comparison of complaints handling that in relation to the Telecommunications Act, Spam Act, and the Do Not Call Register Act that complaints are resolved quickly and efficiently. Although the TIO has established timeframes for members of the TIO Scheme to respond and to resolve complaints at each stage of its complaint handling process, it has not set out a similar timeframe that is transparent for complainants or the TIO Scheme itself.  

One of the continuing problems in relation to privacy complaints is that there may be different outcomes when regulators have overlapping jurisdiction such as under industry codes such as the TCP Code and the e-marketing Code (see discussion below at [8.4.2]). Complaining to one regulator may preclude complaining to another. Also if there is a privacy issue under a specific industry code with an approved privacy code such as the TCP Code or e-Marketing Code then an individual cannot complain to the Australian Information Commissioner about organisations that are bound by the TCP Code or e-Marketing Code.  

The problem of overlapping jurisdictions is evident from the cases involving Telstra Corporation Ltd., and Vodafone Hutchinson Australia (Vodafone). These concerned allegations that the companies had compromised customer’s personal information. In the case of Vodafone, customer details were on the Internet; users with a password were able to log on to the portal from anywhere and access any customer’s details. Personal details (including names, home addresses, driving licence numbers, and credit card details) of

139 Refer to chapter 7 at [7.4]-[7.4.4]; See also above at [8.2.2] in relation to complaints handled by industry regulators and also above at [8.2.1] for the complaints part provided under the Privacy Act 1988 (Cth).  
140 Privacy Act 1988 (Cth) s 36 (1A); See also above at [8.2.1].  
millions of Vodafone customers were made publically available on the internet. This is a major breach of the telecommunications service provider’s privacy obligations to ensure data security.

Similarly, in October 2010, Telstra disclosed that certain customer details affecting 220,000 customers had inadvertently been disclosed to other customers following a mail-merge error. The complaints against Telstra and Vodafone were dealt with by the former Privacy Commissioner (now Australian Information Commissioner) and ACMA. The Privacy Commissioner initiated an own motion investigation into the allegation that Vodafone had breached data security provisions. The Privacy Commissioner found that the allegations were not substantiated and that Vodafone had not breached NPP2.1 and NPP4.1. Similarly in the case of the Telstra Corporation Limited, the PC found that the allegations against Telstra were not substantiated. The ACMA exercised its broader powers to investigate systemic risks by writing to Telstra Corporation and Vodafone Hutchinson Australia to submit for further investigations. The ACMA also requested information from the Top 10 telecommunications service providers (based on TIO complaints) on the measures that each provider has in place to safeguard the personal information of customers and the adequacy of measures taken. This highlights the limited powers of the Information Commissioner under the Privacy Act in comparison to the wider powers of the ACMA.

For effective complaint handling there needs to be consistent processes and, outcomes between regulators for resolving privacy complaints. If a complainant is seeking
compensation or an apology,\textsuperscript{151} and if the complaint is not resolved by the provider, the avenue for complaint is the TIO but not the ACMA. The latter has no power to order compensation.

The overlapping roles of industry regulators and the Australian Information Commissioner create difficulties in providing a coherent approach to protection and enforcement of the e-commerce user’s privacy. One approach is to vest jurisdiction in the Australian Information Commissioner to deal with all privacy related complaints. The powers of the Australian Information Commissioner should be increased to allow greater monitoring and investigation of systemic risks such as now exists in the ACMA. Accompanying this increase in jurisdiction, the Office must be given sufficient resources to carry out these obligations. This doesn’t mean that the advantages of industry based dispute resolution schemes will be lost; but rather these will fit under the umbrella of the Australian Information Commissioner rather than under a different regulatory authority. But there are some disadvantages to this approach. One such disadvantage is that the Australian Information Commissioner is an individual, independent regulator and not a regulatory agency or a commission such as the ACMA.\textsuperscript{152} There is also a possibility that an individual independent regulator may be subject to political pressures or there may be a lack of accountability.\textsuperscript{153}

The next section examines if there is compliance with the current framework under the NPPs and industry codes under the TCP Code and the e-Marketing Code.

\section*{8.3 Compliance}

An important aspect to ensuring compliance with the information privacy regulatory framework is to monitor and audit organisations for privacy compliance and then to have appropriate mechanisms for enforcing compliance. The next section examines first if there is compliance with the Privacy Act NPPs and then under the TCP Code and the e-Marketing Code; and secondly the factors that may inhibit compliance.

\textsuperscript{151} Refer to discussion on remedies below in [8.4].
\textsuperscript{152} Privacy Act s 26A provides that the Privacy Commissioner is the Head of a statutory Agency.

174
8.3.1 Compliance with Privacy Act NPPs

In relation to compliance, the key areas for concern are whether data collectors: (1) comply with the NPP or code requirements relating to data collection, use and/or disclosure to third parties; (2) provide data subjects access to and correction of inaccurate personal; (3) ensure data security and notification of data security breach.

The Office of the Australian Information Commissioner adopts a light touch regulatory response that compliance will be best achieved through helping organisations to comply rather than to seek out and punish those organisations that do not comply with fair information practices under the NPPs. The Australian Information Commissioner publishes an Annual Report, and case notes on decisions on the issues and outcomes of selected complaints to provide insights into how privacy principles are being applied. This is aimed at assisting complainants to decide if complaints should be pursued; for organisations to know if they are complying with the NPPs and if personal information is being handled appropriately and to encourage good privacy practices and compliance with the Privacy Act; and finally provide accountability and transparency in the investigation process and decision making by the Office of the Australian Information Commissioner. The Commissioner also encourages organisations to make systemic changes to systems and practices and provide community education. The Commissioner provides guidance about the investigation process to complainants with the focus on conciliation. As previously noted above in [8.2.1], there were no determinations made by the former Privacy Commissioner during the period 2005-11.

8.3.1.1 Evidence of compliance with NPPs

Private sector organisations argue that there are very few written complaints relative to the number of transactions that take place daily within Australia and across borders (see Table

156 Privacy Act 1988 (Cth) s 27(1) (m).
157 For further details refer to the Office Australian Information Commissioner Website for complaints process <http://www.oaic.gov.au>.
158 See Office of the Privacy Commissioner’s Annual Report for the years 1 July 2005- 30 June 2010; Office of the Australian Information Commissioner’s Annual Report for the year 1 July 2010- 30 June 2011; See also Cyberspace Law and Policy Centre, above n 87, 21.
8.2 above). But it appears that although the NPPs have been in place since 2001, there is a lack of understanding of the NPPs. This is evident from the high percentage of enquiries from individuals\(^{159}\) and concerned private sector industry groups.\(^{160}\) The low levels of complaints do not necessarily indicate positive evidence of satisfactory levels of privacy compliance with the NPPs by a majority of private sector organisations.\(^{161}\) Explanations for the low levels of complaint\(^{162}\) have been referred to above in [8.2.1.1]. The evidence is that dissatisfied consumers rarely complain and it is likely to be no different in relation to privacy matters.

**8.3.1.2 Monitoring and auditing for compliance**

The problem is that without proper monitoring and auditing, the level of compliance with the NPPs by organisations is unknown. Independently of this, the complexity of the system may itself not assist compliance. Chapter 6 at [6.2.1.2] has alluded to the difficulties for small businesses about their compliance obligations when they are exempt from the NPPs but may be bound by privacy codes under telecommunications and other legislation.\(^{163}\)

**8.3.1.3 Costs of compliance**

Another factor that may be relevant to achieving compliance is the cost of compliance. Cost of compliance for businesses is one of the main arguments in favour of retaining the small business exemption under the Privacy Act.\(^{164}\) ‘Compliance costs’ are ‘the direct costs to businesses of performing the various tasks associated with complying with government regulation’.\(^{165}\) In the submissions to the Information Commissioner for its review of the Privacy Act, private sector organisations have cited cost of compliance as one of the reasons for a lack of compliance.\(^{166}\) The costs for small business have been referred to in chapter 6 at [6.2.1.2]. Web data collectors are forced to dedicate ever-increasing attention

---

\(^{159}\) Office of the Privacy Commissioner, above n 107, 46.

\(^{160}\) Ibid 48.

\(^{161}\) Office of the Privacy Commissioner, above n 96, 132.

\(^{162}\) See the submission made by the Australian Finance Conference, the ANZ Bank, the Insurance Council of Australia, Optus, and the Financial Planning Association.

\(^{163}\) Refer to Tables 8.1, 8.3 above.


\(^{166}\) Australian Law Reform Commission, above n 97, 26.

\(^{166}\) Office of the Privacy Commissioner, above n 96, 148.
and resources to privacy protection for their customers with respect to implementing privacy legislation including developing and recording systems, developing policies and procedures, and staff training. The compliance costs to businesses include: for example informing individuals from whom personal information has been collected; seeking consent for use and disclosure of information for secondary purposes; and providing individuals access to their personal information. Those businesses that comply incur compliance costs while the non-compliant ignore it and ‘free ride’. Cost of compliance may vary from one industry to another and are affected by different regulatory requirements that provide for the development of industry codes.\footnote{Privacy Act 1988 (Cth) s18BB; Telecommunications Act 1997 (Cth) s 107; Spam Act 2003 (Cth)) s 3 provides that the Telecommunications Act 1997 (Cth) contains additional provisions about commercial electronic messages. Those provisions include pt 6 (industry codes and standards), pt 26 (investigations), pt 27 (information-gathering powers), and pt 28 (enforcement).}

It is difficult to estimate the cost of providing effective information privacy.\footnote{Office of the Privacy Commissioner, above n 96, 172.} Costs of compliance should be broadly measured in terms of the trade-off between costs and the benefits of compliance.\footnote{The Taskforce on Reducing Regulatory Burdens on Businesses in 2006 made recommendations to the Australian Government to consider the impact of privacy requirements on business compliance costs in the context of a wider review of Australian privacy laws.}

Simple cost benefit analysis fails to take into account the value of brand equity or public reputation that major companies invest in heavily.\footnote{It does not decide how much individuals are willing to pay for their privacy. See Blair Stewart, ‘The Economics of Data Privacy: Should we place a dollar value on personal autonomy and dignity?’ (2004).} There is evidence that the financial, banking and the insurance sectors have invested a lot of attention and resources in ensuring privacy compliance as a necessary part of its business operations.\footnote{Refer to submission by Coles Myer Ltd in Office of the Privacy Commissioner’s, above n 96, 174.}

More often the right to privacy protection is balanced against commercial interests. The cost of privacy compliance should be regarded as simply a cost of doing business in the same way as compliance with legal obligations such as occupational health and safety. Moreover if these businesses trade with businesses in EU Member States then they will have to comply with EU standards or equivalent standards. But as argued in chapter 3 [3.3.2], if privacy is a human right, then it is not to be traded off against commercial interests. This is because the human right of privacy is necessary for meaningful

\footnote{The ANZ Bank submitted that the differing state and territory workplace surveillance laws add to compliance cost and complexity. See Office of the Privacy Commissioner, above n 96, 146.}
democratic participation, human dignity, autonomy and equality of respect. If privacy is considered a human right, then the state must ensure that the commercial interests of e-commerce providers are not offset against the e-commerce user’s right to privacy.

A further factor which may affect compliance is the absence in the Privacy Act of a requirement for mandatory prior registration of all data collectors, and notification of data collection prior to data collection as currently required under the EU Directive. This makes it difficult for the Information Commissioner to monitor compliance. Statistics on the failure to notify the individual about the way private sector organisations process personal information or to make necessary changes to their notification entry were not reported by the Office of the Australian Information Commissioner in its Annual Report for the financial years 2008-10. So the evidence is lacking that organisations actually comply with the NPPs. It is suggested that for the Privacy Act to be effective it should adopt an effective audit, monitoring or verification strategy. Only then can the level of compliance with the NPPs be assessed. This contrasts with duty to notify prior to collection in the EU discussed in chapter 5 at [5.3.2.3]. It has also previously been noted in chapter 5 at [5.3.2.5], that there is now a shift in the European Union approach with an emphasis on verification.

A further factor relevant to compliance relates to the risk of penalties or sanctions. If there is a low risk of penalty or sanction, there is less incentive for compliance. The risk of sanctions and penalties are relatively low. First because the level of written complaints is low and very few cases attract substantial penalties or remedies (see Table 8.8). Where the risk is low, compliance is likely to be given lower priority than such matters as taxation and more immediate regulatory concerns for private sector organisations. Although the Australian Information Commissioner can audit non-exempt data collectors, an audit is

---

173 For further details on Immanuel Kant (1724-1804) and his fundamental idea of ‘critical philosophy’ on human autonomy see Kant’s most notable written and published works that include: The Critique of Pure Reason (2nd ed., 1787) (translated by Norman Kemp Smith, Palgrave Mcmillan, 1st ed, 1929, 2nd ed, 1933); The Foundation of the Metaphysical of Morals or Groundwork of the Metaphysics of Morals (German: Grundlegung zur Metaphysik der Sitten, 1785) (translated by H J Raton, Cambridge University Press, 1996); the Critique of Practical Reason (1788) (translated by Thomas Kingsmill Abbott, Longmans, Green, 1st ed 1909) (Dover Philosophical Classics, 1st ed, 2004).
174 Refer to discussion in chapter 5 [5.3.2.3].
175 The Australian Information Commissioner has limited power to audit public sector agencies. See Privacy Act 1988 (Cth) s 27 (1) (h), s 27 (1) (ha), s 28 (1) (d)-(f).
undertaken only if organisations request an audit. It is usual for the Office of the Australian Information Commissioner to become aware of non-compliance through complaints from individuals, the organisations concerned, or the media rather than through its own investigatory procedures. The Australian Information Commissioner appears not have the resources or power to audit and monitor compliance with the NPPs, (see chapter 7 at [7.2]). Without the ability to conduct mandatory audits, the Commissioner is restricted in its ability to protect e-commerce users’ privacy. The problems are compounded by the Commissioner’s lack of power to require private sector organisations to report on their compliance. Nor does the Australian Information Commissioner have the power to carry out random checks on private sector organisations to see if they are complying with the NPPs. This is in contrast with the ACMA’s monitoring powers that enable it to audit registered suppliers under the suppliers auditing program for compliance with surveillance principles. The ACMA’s compliance strategy is based on mandatory reporting, sample audits of compliance and complaints. As soon as a complaint has been lodged for a breach of the TCP code, or the e-marketing code ACMA focuses on monitoring for example a telemarketer or fax marketeer for compliance with the do Not Call Register Act and industry standards. As previously noted in chapter 5 at [5.3.2.3], and in contrast to the provisions under the Privacy Act, it is mandatory for data collectors to notify the supervisory authority in EU Member States prior to data processing unless the exceptions apply. The 2012 reform proposals, in addition require a data controller to notify the supervisory authority and the data subject whether it is intended to transfer data to a third country and the level of protection available in that third country, art 14(1)(g). These measures enhance the powers of the supervisory authority

176 The Australian Information Commissioner does not have an audit function in relation with compliance with the NPPs by a private sector organization unless requested by the organization under Privacy Act 1988 (Cth) s 27(3).
178 Office of the Privacy Commissioner, above n 96, 146; Australian Law Reform Commission, above n 97, 1522.
179 Office of the Privacy Commissioner, above n 107.
182 Ibid, 97-98.
183 See European Commission, Proposals for a Regulation of the European parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) Brussels, 25 January 2012 COM(2012) 11 final 2012/0011 (COD). The 2012 reform proposals set out some exceptions to prior notification of data collection in art 14(5) such as where the data subject already has the information referred to in art 10 of Directive 95/46/EC above; if the
to monitor compliance with the EU’s data protection regulation. Consequently, unless the Commissioner is given adequate resources and legislative powers under the Privacy Act to monitor compliance and investigate breaches of NPPs it will be difficult for the Australian Information Commissioner to determine whether there is compliance with NPPs.

Finally, there is serious difficulty in monitoring compliance in relation to transborder transactions. This is particularly the case as there is no requirement to issue notice of collection, use and/or disclosure and/or a data security breach notification.\(^{184}\) Monitoring compliance with the data security breach notification is difficult in transborder flows of personal information as there is difficulty in tracing data over different jurisdictions. The difficulties are compounded in e-commerce transactions as e-commerce users may not provide their original email address or overseas address and this makes it impractical for data collectors to issue notices under the NPPs. However this problem can be resolved through timely and swift public notice through emails, media release, and warnings on websites to customers and users that there has been a data security breach.\(^{185}\) It is remarkable that in Australia there is no specific obligation to inform e-commerce users of data security breaches.\(^{186}\) There is only a Guideline relating to data security breaches.\(^{187}\) The Guide aims to provide general guidance on key measures that organisations can consider when responding to a personal information security breach.\(^{188}\) Since guidelines are not binding, the privacy of e-commerce users cannot be assured.

The sections following examine compliance under the two industry codes, the TCP Code and the e-Marketing Code.

\(^{184}\) Australian Law Reform Commission, above n 97 [51]; Office of the Privacy Commissioner, ‘Submission to Senate Environment and Communications Reference Committee: The adequacy of protections for the privacy of Australians online’ (April 2011), Submissions 16, 19.

\(^{185}\) Conrad Walters, ‘Consumers Have a Right to be Told of the Dangers’, The Sydney Morning Herald, (Sydney, 8 April 2011) 11.


\(^{187}\) Ibid.

\(^{188}\) Ibid.
8.3.2 Compliance with the TCP Code and the E-marketing Code

Compliance with approved codes is voluntary unless otherwise directed by the ACMA. Under Telecommunications Act s 122, the ACMA can issue formal warnings if the ‘person’ that is a participant in a particular section of the telecommunications, e-marketing, telemarketing or the fax marketing industries, contravenes an industry code registered under the Industry Code of conduct. Under the Telecommunications Act, s 122 (3) if ACMA is satisfied that there is a contravention of the industry code which relates directly or indirectly to a matter dealt with by the NPPs (as provided under Privacy Act Part IIIAA ss 18BA-18BI), or by an approved privacy code under the Telecommunications Act, then ACMA must consult the Australian Information Commissioner before issuing a formal warning. Besides information from the Australian Information Commissioner, the ACMA considers information provided by a number of sources such as the Consumer Consultative Forum, individual consumers, media reports, and reports from telecommunications service providers including information provided by TIO when it undertakes its compliance and enforcement function.

The ACMA’s compliance strategy is based on mandatory reporting, sample audits of compliance and complaints. This contrasts with the Privacy Act that does not give power to the Information Commissioner to monitor compliance. Consequently in relation to the telecommunications industry, the ACMA as the code regulator has much greater powers to monitoring compliance with the Code and as such there is likely to be greater accountability and compliance by those bound by the Code.

The next section examines if there is compliance under industry codes of practice, in particular under the TCP Code and the e-Marketing Code.

8.3.2.1 Level of Compliance – TCP Code and e-Marketing Code

The ACMA has commented that there is no widespread code compliance among service providers so that it appears that commercial and regulatory incentives to comply are

---

189 Telecommunications Act 1997 (Cth) s 121.
190 Australian Communications and Media Authority (ACMA), above n 119, 4. ACMA can request a telecommunications service provider to submit detailed quarterly reports against internal complaint-handling requirements of the TCP Code.
ineffective. But this needs to be viewed in the context of the types of complaints that are received. The TIO’s statistics for December 2010 and January 2011 show an increase in complaints. The TIO received a total of 197,682 new complaints, a 17.8 per cent increase from the previous year. The TIO recorded a total of 4653 confirmed code breaches during 2010-11 by 122 different service providers out of which 4634 related to the TCP Code. Between July 2010 and June 2011, the TIO monitored over 100 systemic issues and intervened in more than 50 matters to avert problems for large number of consumers. But these system issues and complaints are mostly concerned with service and product delivery with quite small numbers related to privacy issues.

The earlier part of this chapter referred to the issues related to unauthorised disclosure of private information by Vodafone and Telstra (see above in [8.2.2.1]). The ACMA was concerned that the incidents may have been symptomatic of a broader problem. It undertook three audits of providers’ websites reviewing information provided to consumers on broadband, post-paid mobile and prepaid mobile products from December 2010 – February 2011. The ACMA requested information from the Top 10 providers (based on TIO complaints) on the measures that each has in place to safeguard the personal information of customers and the adequacy of these measures. So that the ACMA has adequate powers to audit and monitor privacy risks to e-commerce providers. The lack of similar powers in the Australian Information Commissioner has already been noted.

The principal reasons for the lack of compliance with the TCP Code and the e-Marketing Code industry Codes is the complexity, and cost of compliance. It has been noted earlier that small business particularly are affected (see chapter 6 at [6.2.1.2]).

In relation to the telecommunications sector the compliance burden may be diminished by combining the various legislation into a single act that applies to all data collectors. There are benefits to organisations if they comply. The benefits from compliance with the e-

---

192 See Australian Communications and Media Authority, ‘Reconnecting the Customer Progress Report’, December 2010; see also Australian Communications and Media Authority, ‘Reconnecting the Customer: Final Public Inquiry Report’ (September 2011) 25.
194 Ibid.
195 Ibid, 11-12.
196 The matters investigated relate to credit management (over-commitment, issues around usage meters), sales practices (telemarketing practices and misrepresentations, advertising, online sign up processes), mobile networks coverage, drop outs, roaming charges, billing (new products and services, mobile SMS charges, billing format). Telecommunications Industry Ombudsman ‘2011 Annual Report’ (2011) 11.
197 Australian Communications and Media Authority, above n 119.
Marketing Code include a decrease in complaints,\textsuperscript{198} and improved customer confidence.\textsuperscript{199} The anticipated benefits to consumers from compliance with the code are that:

- consumers can expect appropriate industry behaviour and obtaining consent prior to sending commercial electronic messaging;
- a reduction in the incidence of unsolicited commercial messages sent by industry members;
- a clear understanding of the e-marketing processes and standards related to commercial electronic messages;
- a clear and transparent means of unsubscribing to and withdrawing consent to receiving e-marketing messages;
- an efficient complaints handling process.\textsuperscript{200}

This next section examines if there is effective enforcement of the NPPs and industry codes.

\textbf{8.4 Remedies and Enforcement}

Complaints handling and outcomes are discussed above in [8.2.1]; [8.2.2]. They illustrate some significant limitations of the enforcement regime under the Privacy Act, and under industry codes. In relation to the NPPs, the statistics on telephone and written enquiries and written complaints indicate that more than 50 percent of written complaints have been dismissed without a hearing (see above in [8.2.1.1]; Table 8.3). As noted earlier under the Privacy Act all claims were settled by conciliation rather than by a determination, (see above in [8.2.1.1]). There is no data available on whether e-commerce users are satisfied with conciliated outcomes. As noted earlier it is telling that the former Privacy Commissioner did not make a single determination during his period in office.

The sections following examine enforcement of the Privacy Act NPPs, and the two approved industry codes under the Telecommunications Act, and Spam Act.

\textsuperscript{198} Refer to the statistics on complaints received in Table 8.5, and the statistics for outcome of investigation in Table 8.8 in relation to the Spam Act 2003 (Cth).
\textsuperscript{200} Australian Communications Authority (ACA), ‘Australian e-Marketing Code of Practice’ (2005) 8. The ACA has since merged under the Australian Communications and Media Authority.
8.4.1 Privacy Act

Another key function of the Australian Information Commissioner is to enforce compliance with the Privacy Act and NPPs. In respect to the NPPs, enforcement of the NPPs first requires a determination by the Australian Information Commissioner under Privacy Act, s 52 or an approved privacy code. The Privacy Act s 52 provides that after investigating a complaint the Australian Information Commissioner may make:

a) a determination to dismiss the complaint, or make a determination for a declaration that the respondent in the matter should not engage in the conduct constituting an interference with the privacy of the individual,

b) declare that the respondent should perform any reasonable act or course of conduct to redress any loss or damage suffered by the complainant,

c) declare that the complainant is entitled to a specified amount by way of compensation for any loss or damage suffered by reason of the act or practice that is the subject of the complaint, and

d) declare that it would be inappropriate for any further action to be taken in the matter.

The Australian Information Commissioners can make a determination declaring that an organisation has obligations not to repeat or continue conduct that is covered by a declaration that is included in the determination and must perform the act or course of conduct that is covered by the declaration.

Enforcement of a determination made by the Commissioner is provided by the Privacy Act ss 54-55. Section 54 provides that a determination made by the Commissioner under s 52 and an adjudicator for an approved privacy code in relation to a complaint under the code is enforceable. Section 55 (1), (2) of the Privacy Act provides for obligations of respondents when a determination is made which can include that such organisations must not repeat or continue conduct that is covered by a declaration; and must perform the act or course of conduct that is covered by a declaration in the determination made by the Commissioner. Under Privacy Act s 55A proceedings may be brought before the Federal Court or Federal Magistrates Court to enforce a determination.

---

201 Refer to discussion above at [8.2.1]). Currently there are only three privacy codes approved by the former Privacy Commissioner under the privacy act.

202 Privacy Act 1988 (Cth) s 55. But the Australian Information Commissioner cannot specify how a particular organisation should comply with the NPPs.
Enforcement of determinations by the Commissioner requires Court proceedings for enforcement. If the complainant commences proceedings in the Federal Court, or the Federal magistrates Court for an order to enforce a determination, (s 55A) there will be a cost to the complainant that may discourage complainants to pursue a remedy for a breach of the NPPs (or industry codes approved under the Privacy Act) by e-commerce users. The reason for this is that there is a constitutional barrier which prevents federal non-judicial bodies from enforcing determinations. Although in theory this may act as a barrier to an e-commerce user’s enforcement of privacy protection, the reality is that resort to Court enforcement will not be necessary if conciliation processes work effectively and are given effect to by the provider. Resorting to Court enforcement has not proven necessary for determinations relating to the Telecommunications Industry.

Where the Australian Information Commissioner investigates a complaint, possible outcomes include the amendment of records, apology, changes to current procedures, provision of access, monetary or other compensation to redress actual loss or damage and, where appropriate, that the organisation provide staff training and counselling. Besides this, the Commissioner also has powers under s 98 to seek an injunction from the Federal Court to ensure compliance with the Privacy Act. An injunction may prohibit an organisation from engaging in conduct that would breach the Act or require it to take steps to being itself into compliance with the Act. This step would only be taken when other more informal means failed to yield a satisfactory outcome. But it appears that neither the former Privacy Commissioner nor the current Australian Information Commissioner have ever sought an injunction to date. This is in contrast to the ACMA that took enforcement action against FHT Travel which included a penalty of $120,000 and sought an injunction against the sole director of FHT Travel in the Federal Court for the first time under the Do Not Call Register Act (see Table 8.10 below). Independently of a determination, settlement by conciliation may result in recommendations for compensation. Table 8.8 following sets out the details.

---

Table 8.8: Outcomes after the Close of Investigations by the OPC for 2008-10, and the OAIC for 2010-11

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Complaints Closed With Remedies &amp; Outcomes</td>
<td>NPPs</td>
<td>Non NPPs</td>
<td>NPPs</td>
<td>Non NPPs</td>
</tr>
<tr>
<td>Records amended</td>
<td>16</td>
<td>3</td>
<td>13</td>
<td>2</td>
</tr>
<tr>
<td>Apology</td>
<td>22</td>
<td>5</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Other remedy (include staff training &amp; counseling etc.)</td>
<td>12</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Compensation up to $1000</td>
<td>20</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Compensation $1001-$5000</td>
<td>12</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Compensation $5001-10,000</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Compensation $10,001+</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Compensation - Confidential Settlement</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total with remedies NPPs &amp; Non NPPs</td>
<td>289</td>
<td>192</td>
<td>155</td>
<td>633</td>
</tr>
</tbody>
</table>

(Source: Table 8.8 - Created by author).

The approach in Australia for dealing with breaches of the NPPs is structured to be low cost, time effective and a non-adversarial, conciliatory approach in settling grievances. The focus is on dispute resolution through the Information Commissioner. It has already been noted above in [8.2.1] that in the period 2005-2011 the Commissioner issued no determinations. This might suggest that conciliation always works. There are alternative

---

explanations particularly where very, very few inquiries result in written complaints, discussed above in [8.2.1.1]. Currently the powers of the Commissioner are limited under the Privacy Act as it only gives power to make determinations on individual complaints, (see above in [8.2.1.1]). It has been noted earlier that the Commissioner does not having a monitoring role in relation to the NPPs or Industry Codes approved under the Privacy Act.

The light touch approach of the previous Privacy Commissioner resulted in no formal determinations during that term of office. When this is added to the lack of powers to audit, monitor and deal with systemic risks, referred to earlier, the Office of the Privacy Commissioner (as it was previously discussed above in [8.2.1.1]), was not an active force in ensuring compliance with the NPPs and industry codes under its supervision. To increase the effectiveness of the work of the then Privacy Commissioner and of the office of the Privacy Commissioner submissions made to the Australian Law Reform Commission suggest that the powers of the Privacy Commissioner should be extended to issue a standard or binding code dealing with systemic issues.

There are no criminal penalties under the Privacy Act when privacy invasive technology is used for data mining, behavioural tracking, and accessed for criminal activities such as identity theft and ‘botnets’. This contrasts with the civil penalty provisions available under the Telecommunications Act, and the Spam Act (see below in [8.4.2]), which arguably provide much stronger deterrents and more effective remedies against privacy invasion. These are supplemented by amendments to the Commonwealth Criminal Code imposing criminal penalties in relation to telecommunications.

The Australian position is in stark contrast to the position in the EU. Article 22 of the Directive 95/46/EC provides that Member States shall provide for “the right of every

207 Office of the Australian Information Commissioner, ‘Privacy Law Reform: Challenges and Opportunities’, (23 February 2012); Australian Law Reform Commission, above n 97, 1518.

208 Australian Law Reform Commission (ALRC), ‘Enhancing National Privacy Protection, Australian Government First Stage Response to the ALRC Final Report 108: For your Information: Australian Privacy Law and Practice’, (October 2009). See Recommendation 48-1 which recommends that pt IIIAA Privacy Act 1988 (Cth) be amended to specify that a privacy code: (a) approved under pt IIIAA operates in addition to the model Unified Privacy Principles (UPPs) and does not replace those principles; and (b) may provide guidance or standards on how any one or more of the model UPPs should be applied, or are to be complied with, by the organisation bound by the code, as long as such guidance or standards contained obligations that, overall, are at least the equivalent of all the obligations set out in those principles.

209 ‘Botnets’ allow computers to be controlled by an unauthorised person or organisation. See the remedies and outcomes provided under the Privacy Act that is reflected in Table 8.8 above.

210 The provisions are contained in Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Act (No.2) 2004 (Cth) amending the Criminal Code 1995 (Cth).
person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the process in question”. Article 23 provides that if any person has suffered damage due to an unlawful processing operation or any act incompatible with the national provisions adopted, then that person shall be entitled to receive compensation from the controller for the damage suffered. Article 24 further provides that a suitable measure must be adopted to fully implement the sanctions to be imposed in case of infringement of the provisions adopted under EC Directive 95/46/EC. It is argued that an Australian e-commerce user should have similar rights. The Privacy Act as currently enacted does not act as a deterrence against privacy breaches. Greater deterrence could be achieved by imposing similar sanctions and civil penalties such as those provided under the Telecommunications Act and the Spam Act.

The next section examines enforcement under industry codes and the provisions for remedies and sanctions under the Telecommunications Act, and Spam Act that regulate the TPC Code and the E-marketing Code. It focuses on civil remedies available to the e-commerce user under the Privacy Act, Telecommunications Act, and the Spam Act.

8.4.2 TCP Code, and E-marketing Code

When a code is registered with the ACMA, such as the TCP Code and the E-marketing Code, the ACMA can take action to direct compliance with the code. 211 The Telecommunications Act s 121(1) provides that if a person is a participant in a particular section of the telecommunications, e-marketing industry, telemarketing or the fax marketing industry, and if the ACMA is satisfied that the person has contravened or is contravening an industry code that is registered under Part 6 relating to Industry Code and Industry Standards, then the ACMA may, by written notice given to the person, direct the person to comply with the industry code. If the ACMA is satisfied that the contravention of the industry code relates directly or indirectly to a matter dealt with by the National Privacy Principles (NPPs) (as defined in the Privacy Act 1988) or by an approved privacy code (as defined in that Act), the ACMA must consult the Australian Information Commissioner before giving the direction. The penalty for non-compliance with an industry code registered under s 121 Telecommunications Act is a civil penalty provision. The Telecommunications Act pt 31B provides for pecuniary penalties for breaches of civil

211 Telecommunications Act 1997 s 136 provides for registration of telecommunications industry code with the Australian Communications and Media Authority (ACMA).
penalty provisions. There is also provision for infringement notices with requisite penalties.  

Section s 132 of the Telecommunications (Consumer Protection & Service Standards) Act 1999 (Cth) requires a telecommunications service provider to comply with the TIO scheme. The TIO refers any non-compliance by a service provider under the TIO scheme to the ACMA for enforcement for breach of the TCP Code. However the TIO investigations provide important information and evidence without which ACMA will not be able to take action for non-compliance with the TCP Code. The TIO report also states that a vast majority of service providers comply. 

New complaints received by the TIO are categorised as Level 1. The TIO refers new complaints to be resolved by the service provider within 30 days without the TIO’s involvement. If the complaint is not resolved within the 30 day period, then the complaint progresses to Level 2 at which stage the TIO steps in to conciliate. Those cases that are not resolved at Level 2 and that may need further investigation by the TIO at Level 3. This is where the TIO provides advice about a fair outcome. At Level 3 the TIO may also make binding decisions if the value of the dispute is below $1,200. Those cases not resolved at Level 3 then progress on to Level 4 at which stage a thorough and detailed investigation is undertaken by the TIO and may result in a binding decision or direction by the TIO. The TIO can issue binding determinations up to a value of $30,000 if a complainant is not resolved through the TIO process of referral, or conciliation, or investigation. Table 8.9 below provides statistics on the number of new complaints received for the reporting years 2009-11 and the number of complaints conciliated determinations made by TIO and referred to the ACMA.

212 Part 31B confers on ACMA the power to declare by legislative instrument provisions that are ‘listed infringement notice provisions’. ACMA can list provisions in a declaration which are eligible for an infringement notice. An infringement notice offers a person the chance to avoid being subject to lengthy and potentially costly court action by paying the penalty specified in the notice. The infringement notice sets out a brief detail of the alleged contravention, the penalty and the period the penalty is to be paid.

213 The TIO has only made 9 referrals to ACMA in the year 2010-2011. The referrals relate to four different service providers who failed to comply with the TIO’s determinations. See the Telecommunications Industry Ombudsman’s, ‘2011 Annual Report’ (2011) 13.

### Table 8.9: Outcomes after Close of Investigations by the TIO for Years 2008-11

<table>
<thead>
<tr>
<th>Complaints statistics (1 July-30 June)</th>
<th>2008-2009</th>
<th>2009-2010</th>
<th>2010-2011</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 1 - New Complaints</td>
<td>175,946</td>
<td>167,772</td>
<td>197,682</td>
</tr>
<tr>
<td>Level 2 - Conciliation</td>
<td>17,391</td>
<td>20,013</td>
<td>17,863</td>
</tr>
<tr>
<td>Level 3 - Referrals to ACMA</td>
<td>4,321</td>
<td>3,791</td>
<td>2,415</td>
</tr>
<tr>
<td>Level 4 - Determinations by TIO</td>
<td>440</td>
<td>413</td>
<td>357</td>
</tr>
</tbody>
</table>

(Source: Table 8.9 - Created by author).

Outcomes for individual complainants under the TCP Code when matters are resolved include: an apology, free service, minor financial compensation, the correction and removal of personal information, credits on bills, re-connection of services, and the correction of inaccurate credit reports.

Although the TIO is the principal avenue for privacy complaints arising out of breaches of the TCP code. In relation to information privacy, Table 8.5 above indicates the total privacy related complaints received by the TIO and Table 8.6 indicates the total privacy complaints investigated by the TIO during the period 2008-11. To date the complaints received by the TIO have largely involved service delivery issues rather than privacy issues. Detailed statistics on the breakdown of outcomes for individuals is not available in the TIO’s Annual Report 2009-11. The outcomes for privacy related complaints under the TCP Code is likely include an apology, an apology, free service, minor financial compensation, or the correction and removal of personal information.

According to the TIO’s Annual Report 2010-11, compensation and reimbursement to complainants vary from customer to customer and there appears to be no fixed amount set for compensation and reimbursements. For example determinations made by the TIO in 2010-11 in relation to telecommunications service providers indicate that determinations

---

216 The source of the statistics in Table 8.9 is the Telecommunications Industry Ombudsman’s ‘2011 Annual Report’ (2011) 29.
218 The TIO has monitored over 100 systemic issues and directly intervened in more than 50 to prevent problems for large numbers of consumers Telecommunications Industry Ombudsman, ‘2011 Annual Report (2011) 11.
for payment of compensation and reimbursements to consumers that range between $19,000 and $86.\textsuperscript{219}

The outcomes for businesses that are the targets of complaints include naming of the party in TIO’s aggregate report showing the number of complaints received against the organisation per year.\textsuperscript{220} The use of media releases and naming of organisations provides adverse publicity, public debate, and intervention by government regulator as was the case with Telstra Corporations Ltd., and Vodafone Hutchinson Australia (referred to above).\textsuperscript{221} However the failure by TIO to follow through on undertakings made to consumers to resolve complaints is a significant problem that has been noted in a number of dealings with members.\textsuperscript{222} The TIO makes no binding decisions but resolves matters through conciliation. The conciliation scheme gives telecommunications companies many opportunities to resolve a complaint before it escalates to level 4. The fees charged by the TIO for investigating a complaint categorised as a level one complaints is $250 and for level two category complaint the fees is $300 from July 2011.\textsuperscript{223} It will be in the interest of telecommunications companies to resolve the issues with the complainant as early as possible rather than for the issues to escalate to level 4 investigations.

With respect to E-marketing, the outcomes of complaints handled and investigated by the ACMA differ according to the category of privacy complaints lodged with the ACMA and also the legislation providing the dispute resolution scheme and remedies for breach. In relation to spam, there is significant deterrence provided by the Spam Act. Section 25 of the Spam Act, provides a maximum civil penalty for contravention and s 29 allows orders for forfeiture of profits derived from spam and payment of compensation to those who are victims of spam. The civil penalties include fines up to $1.1 million per day for contravention of the Act.\textsuperscript{224} The Federal Court may make ancillary orders: directing the


\textsuperscript{221} Refer to discussion in [8.2.2.1]; [8.3.2.1 above; See also Telecommunications Industry Ombudsman, ‘Annual Report for 2008-2009’.


\textsuperscript{223} Lucy Battersby, ‘Ombudsman cuts jobs as complaints fall’ The Sydney Morning Herald, Business Day News -Telecoms (Sydney), 28 September 2012, 5.

\textsuperscript{224} Under Spam Act s 25 (5) (b), a penalty unit is at the time of writing $110. So if an organisation with a previous record of spamming and who sent two or more spam messages on a given day without consent is a maximum fine of 10 000 penalty units. This equates to a maximum penalty of $1 100 000.
payment of compensation to a victim of a contravention of a civil penalty provision (s 28); and directing the payment to the Commonwealth of an amount up to the amount of any financial benefit that is attributable to a contravention of a civil penalty provision (s 29).

The Spam Act also gives the ACMA powers to search premises and seize equipment and impose, and enforce penalties. The Spam Act s 32 provides that the Federal Court may grant an injunction in relation to contraventions of civil penalty provisions restraining the person from engaging in the conduct and if the court is of the opinion and if desirable to do so requiring the person to do something. Consequently, it is the associated legislation that provides appropriate enforcement through the imposition of civil penalties.

With respect to businesses that target individuals with spam messages, the ACMA can use its regulatory powers to enforce the provisions of the Spam Act 2003. But as will be seen from the Table 8.10 below, these remedies available through Federal Court proceedings have largely not been utilised. The ACMA is more likely to issue an advisory letter followed by formal warnings and enforceable undertakings as the preferred method of enforcement. These do not involve compensation to the affected individual.

A summary of the enforcement action undertaken by the ACMA in relation to telemarketing and spam during the year 2008-09 and 2009-10 is set out in Table 8.10 below.

---

## Table 8.10: Outcomes after the close of investigations by the ACMA under the E-Marketing Code for 2008-11

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Tele &amp; Fax-marketing</td>
<td>Spams</td>
<td>Spams</td>
<td>Spams</td>
</tr>
<tr>
<td>Advisory/ warning letters</td>
<td>380</td>
<td>967</td>
<td>234</td>
</tr>
<tr>
<td>Investigations</td>
<td>21</td>
<td>25</td>
<td>13</td>
</tr>
<tr>
<td>Formal warnings</td>
<td>6</td>
<td>7</td>
<td>4</td>
</tr>
<tr>
<td>Infringement notices</td>
<td>7</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>Enforceable undertakings</td>
<td>2</td>
<td>2</td>
<td>7</td>
</tr>
<tr>
<td>Civil penalties</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Injunction</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>No findings or decision not to investigate further</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

(Source: Table 8.10 - Created by author).

### 8.4.2.1 Problems in providing effective sanctions and remedies

The problem in providing effective and consistent remedies under the TCP Code, the e-Marketing Code including the Privacy Act generally is that there are variations in procedure, remedies, and sanctions.

Firstly, a number of codes may be applicable to an online transaction at any given time. These codes address a range of matters such as consumer codes, operations codes regulating relationships between service providers; others that regulate technical operations to ensure network connectivity, and those that relate to customer equipment standards. Each Code of Practice has a number of code regulators and adjudicators to administer the codes of practice with overlapping roles and jurisdiction (see chapter 7 at [7.4]). It is a problem for national regulators such as the ACMA and the ACCC. Besides the ACMA, the ACCC has a general power to approve industry codes of practice that are legally enforceable under the Competition and Consumer Act 2010 (see chapter 7 at [7.4]).

---

226 The statistics on remedies and sanctions under the e-Marketing Code has been compiled by the author from statistics provided in the ACMA’s Annual reports for the years 2008-2010. See also Cyberspace Law and Policy Centre, above n 87, 18.

227 Australian Communications and Media Authority, ‘Reconnecting the Customer: ACMA Public Inquiry Consultation Paper’ (July 2010) 5.
[7.4.2]). Where there is a breach of an industry code that may also be a breach of the e-commerce user’s contract giving a right to take legal action for breach of contract. For example an e-business may have misleading privacy policy statements, or unfair contractual terms, or be involved in prohibited sales practices (see chapter 4 at [4.2]). In contrast the ACCC has the power to impose: financial penalties up to $1.1 million for corporations and $220,000 for individuals; banning orders; substantiation notices; infringement notices; refunds and issue public warnings. In respect to industry codes, ASIC generally cannot take enforcement action if a code is breached unless a breach of the law is also involved. But if there is significant non-compliance with an industry code, then ASIC may publicise the breach in some instances.

Secondly, there are also inconsistent approaches to complaint handling both in terms of processes, outcomes, and remedies where multiple regulators are involved. Especially if a complainant is seeking compensation or an apology then they should use the Office of Australian Information Commissioner or TIO rather than the ACMA. The ACMA focuses on changing business conduct and remedies for individuals utilising federal court proceedings are rare.

Thirdly, the “light touch” approach with the preference for conciliation rather than court enforcement may not provide sufficient deterrent for organisations that breach their privacy obligations. It has been noted that although the telecommunications legislation such as the Spam Act, imposes significant penalties, the reality is that the regulator has generally not taken these enforcement measures. The Australian Information Commissioner should be provided powers to use the full range of available civil penalty provisions similar to those available to the ACMA such as injunctions, and enforceable

---

228 Competition and Consumer Act 2010 (Cth) provides for industry code and penalties that can be enforced by the ACCC for contravention of industry codes.
229 Competition and Consumer Act 2010 (Cth) pt II s 6A establish the Australian Competition and Consumer Commission, and pt IVB provides for investigative powers and power to issue public warning notice for contravention of Industry Code.
230 ACMA refers botnet activities to the Australian High Tech Crime Centre, the relevant state or territory police as botnets are an offence under Criminal Code 1995 pt 10.7, ss 477-478.4. Botnets relate to the unauthorised access and modification of data via a carriage service and the penalty for this offence is a two year maximum prison sentence whilst possession of data with intent to commit a computer offence carries a 10 year maximum prison sentence. There is a three year maximum prison sentence for producing, distributing or obtaining data with intent to commit a computer offence such as writing a bot code or selling a bot code or other similar actions. See Australian Communications and Media Authority, ‘Powers and Penalties’ (online) <http://www.acma.gov.au/WEB/STANDARD/pc=PC_1310531>. 194
undertakings besides compensation and apologies to effectively deter breach of the NPPs, and industry privacy codes.

**8.5 Conclusion**

An e-commerce user’s right to privacy is compromised unless effective remedies are available for enforcement. It is clear that under the Privacy Act NPPs and Codes approved under the Privacy Act, the Australian Information Commissioner does not have sufficient powers or resources to monitor, audit or investigate individual complaints or systemic problems. In the absence of these broader powers, it is simply unknown whether there is compliance with the NPPs. There are significant barriers to an e-commerce user obtaining a remedy. In addition to the requirement of a formal written complaint, the Commissioner may refuse to investigate and is under no obligation to make a determination. As noted several times, the former Privacy Commissioner has not exercised what powers it did have to make formal declarations for the period 2005-11 (see above at [8.2.1.1]). Even then in order for a declaration to be enforced the e-commerce user must commence court proceedings. This is in contrasts with the EU provisions which provide a right to redress and effective remedies for the e-commerce user where there is a breach of the user’s privacy, (see chapter 5 at [5.3.2.7). In summary, e-commerce users are seriously hampered in their ability to ensure the protection and enforcement of their rights to privacy under the NPPs.

In contrast to the Privacy Act, it is also apparent that the TCP Code and the E-Marketing Code examined in chapter 7 through the ACMA (see at [7.4.3]), and the TIO provide much more efficient and timely mechanisms for dispute resolution (see at [7.4.4]). Compared to those data collectors who are bound by the NPPs, the enforcement and sanctions for breach of the Spam Act that provide for mandatory compliance appears to be more effective in ensuring protection of information privacy.

In relation to the NPPs, E-commerce providers should be formally required to undergo external audits to verify compliance; and should provide systems to investigate and act upon complaints from customers with advice to e-commerce users how to protect and enforce their privacy rights. It should also provide a contact point within an organisation of the person who is responsible for privacy protection. This is because in respect to complaints about breach of NPPs, the Information Commissioner is not in a position to
know if these problems occur across the board and more specifically how many complaints are made directly to organisations; how many are resolved at that level; and what difficulties individuals encounter in lodging a complaint with the organisation. Currently most private sector organisations do not have a privacy contact officer. One reason for this is that there is no requirement to report a breach of the NPPs. The only requirement is that the organisation must take reasonable steps to protect the personal information it holds from misuse and loss from unauthorised access, modification or disclosure.\textsuperscript{231}

It has been noted, however, that the problem for the e-commerce provider is the multiplicity of regulators that have some role to play in the development, approval and enforcement of industry codes. It is argued that this industry based approach to protection of privacy fails to provide a coherent approach to the protection of privacy for the e-commerce user. Whilst there is value in industry expertise in recognising and responding to privacy issues within that particular sector, there is no reason why this type of expertise could not be embedded within a single Privacy body or Commission. This would give the e-commerce user a single avenue to complain, have issues investigated and obtain uniform remedies under a single regulator.\textsuperscript{232}

The next chapter summarises the findings of this thesis and concludes with some recommendations as to what more needs to be done to provide more adequate and effective information privacy protection for individuals and e-commerce users.

\textsuperscript{231} Privacy Act 1988 (Cth) sch 3 NPP4.1.
\textsuperscript{232} The Australian Communications and Media Authority (ACMA)’s public inquiry has highlighted the sortcomings of the current legislative framework. The preference to industry self-regulation in the current scheme of privacy protection means that regulatory responses are slow and consumer harm can continue much longer than desirable. See Australian Communications and Media Authority (ACMA), ‘Reconnecting the Customer: Final Public Inquiry Report’ (September 2011) 27.
Chapter 9: Concluding Thoughts and Future Directions

9.1 Introduction

This thesis has explored the impact of information technology on privacy, and the threat to e-commerce users from the privacy invasive activities of data collectors. It examined the protection afforded to e-commerce users by Australian federal legislation regulating privacy.¹ The legislation has been evaluated in the light of international approaches to privacy protection particularly the OECD and EU provisions.

This concluding chapter summarises the main findings of this thesis, and how this thesis might contribute to knowledge and research on the future direction of information privacy protection for e-commerce users.

9.2 The Context

The Internet has revolutionised the retail environment and created a digital economy. Information technology and e-commerce have fundamentally transformed the ability to communicate, to access information and transact within a global market. Whilst e-commerce has brought significant advantages to its users offering flexibility and choice, personal information that is collected from or about e-commerce users with or without consent may be used for purposes other than that for which the user had given consent (or where legally required). Information may be shared with and used by unknown third parties without the e-commerce user’s consent. Privacy protection is fundamental to the success of e-commerce and the digital economy. Without privacy protection personal information is put at risk and individuals exposed to identity theft as well as losing control over their personal information. It is thus necessary for data collectors to ensure that personal information is protected from loss, misuse, unauthorised access, disclosure, alteration and destruction. Abuse of personal information are likely to emerge where such information is not adequately safe guarded from wrongful use and disclosure.

¹ State privacy laws have not been considered.
9.3 Privacy and E-commerce Users

Privacy is viewed as an interest in personality, about who the individual is, their sense of self, and how they wish to be viewed by others. It is a right to be left alone, not to have one’s personal information spread to the four winds, or viewed, used or disclosed to others without consent. Privacy is an elusive concept and no single definition has proven to be satisfactory in delimiting what is privacy. The pragmatic approach proposed by Solove has been adopted. Solove suggests that rather than attempting a single unifying definition of privacy to cover all contingencies, it will be more useful to adopt a pragmatic approach to determine which privacy interests and concerns need to be addressed, how they are to be addressed, and in relation to both the relevance of context (see chapter 3 [3.2]) Applying this framework, it becomes clear that the activities of data miners, electronic dossiers, and disclosure and usage of e-commerce users’ personal information infringe the rights and ability of e-commerce users’ to control access to information concerning themselves.

Privacy, it is argued, is a human right as it is fundamental for the existence and dignity of a human being, (see chapter 3 [3.3.2]). This is important because privacy as a human right is not subject to takings by the state and not to be traded off against commercial interests in the name of efficiency or cost. But this is the position under Australian privacy legislation particularly under exemptions granted under the legislation, to small businesses, and transfers to related companies and direct marketing as discussed in chapter 6.

9.4 Privacy, Consent, and Autonomy

This right to privacy recognises that a legally competent person can consent to intrusion in the private sphere so that e-commerce users can waive their right to privacy typically by ticking the box or agreeing to conditions of use. But as argued in chapter 4 this is often perfunctory with e-commerce users given little effective choice. In order for this to be regarded as a true expression of autonomy, e-commerce users must have options whether or not to agree, information must be readily accessible and in language which the ordinary user can comprehend. The assumption that ticking (or unticking) a box is sufficient is out of step with modern consumer protection legislation. Under the Competition and Consumer Act 2010, some protection is given to consumers where there is unequal

---

bargaining between the parties under standard form contracts. Ideally legislation should ensure that constraints on the ability to make informed decisions are removed. This will require at the very least that information is easily accessible and in plain English with opportunities for the consumer to exercise choice in deciding what information is made available and for what purposes.

9.5 International Landscape for Privacy Protection

Chapter 5 examined the OECD and the European Union principles on privacy protection. These principles have been the most influential in providing models for the protection of information privacy. Australia’s privacy legislation and National Privacy Principles are based primarily on the OECD principles. But the higher standards under EU directives have assumed greater importance in establishing international norms, particularly through the regulation of transborder flows of information. The EU directives are particularly important in their recognition of privacy as a human right not subject to takings by the State, an approach that should be adopted in Australia.

9.5.1 The OECD Approach

Although not binding on member nations, the OECD Guidelines shaped and defined privacy protection of many OECD member nations including Australia and represent an international consensus on personal data protection in respect to public and private sectors. The eight OECD principles for the collection and processing of personal data formed the basis for the Australian National Privacy Principles. The OECD Guidelines were first developed thirty years ago and are less effective in enforcing privacy in the online environment. This is due to the current developments in information technologies, the dramatic changes in the volume and uses of personal information, trends in information collection such as data mining and trends in global data flows. Similar limitations exist in the National Privacy Principles modelled on the OECD guidelines. So, for example, newer technologies referred to in chapter 2 such as data mining are not specifically covered by the Guidelines. Although the OECD Guidelines, like the EU directive, require prior registration by data controllers, an approach that is recommended in this chapter, the key problem is that the OECD Guidelines do not provide clear guidelines on what will be expected of data collectors in an accountability system; how the privacy principles will be
enforced; how accountability is to be measured; and how protection of personal data can be ensured. This, in part is a consequence of the nature of the organisation which is based on voluntary international co-operation in establishing policies. This contrasts with the EU approach which has the capacity to bind its members. They provide for greater protection to citizens in relation to trans-border transfers through requirements of prior registration and strong provisions of enforceability, and most importantly by recognising privacy as a human right, all of which together set the standard for privacy protection. Consequently, it is the EU Directives that provides an important model for Australia for privacy protection for e-commerce users.

9.5.2 The EU Approach – Privacy as a Human Right

The EU’s approach to privacy protection gives expression to privacy as a human right which is not traded off against commercial interests unless there is a compelling case to do so.3 Consequently, under the EU directives there is no exemption for small businesses and collection, use and disclosure of personal information are much more tightly controlled. Controllers must currently register prior to information collection and are required to stipulate for what purposes the information will be collected, used and disclosed. Current proposals for reform move away from prior registration to a regime based on verifiable compliance (see chapter 5 [5.3.2.3]). This is much more effective than the relatively weak legislative response under the Privacy Act referred to below.

Under the EU Directives there are also much stronger measures in place to deal with the transfer of personal information out of the EU. Where the laws of the third country do not provide comparable protection for EU citizens, the Directive requires other measures to be taken, including contractual devices which permit an EU citizen affected by the breach to bring a claim based on breach of contract between the controller and the offshore entity. It contrasts with the relatively loose Australian provisions which, in addition to containing significant exceptions as discussed in chapter 6, only requires organisations to have a reasonable belief as to adequate protection in the jurisdiction to which the information is transferred, consent of the individual to the transfer, or the transfer is considered necessary for the performance of a contract between the individual and the organisation.4 In the

3 See the general provisions of the Recitals 1-3 to EC Directive 95/46/EC in Appendix 2.
4 Privacy Act 1988 (Cth) NPP9.
absence of strong mechanisms to monitor and audit, there cannot be high levels of confidence that minimum levels of privacy protection are achieved in Australia.

9.6 Australian Federal Statutory Privacy Protection

The framework for information privacy protection in Australia takes a multi-faceted approach that includes co-regulation by the state and industry sectors. There are many pressing issues arising out of the federal legislation. These include lack of a coherent legislative regime, the failure to respond to a changing technology environment, the preference for efficiency and commercial interests over the e-commerce user’s right to privacy; the weak legislative response to data privacy as well as the relative lack of audit, monitoring and enforceability where there has been a breach of privacy.

9.6.1 Privacy Protection – the Need for a Coherent Approach

The regulation of privacy at the federal level lacks a coherent approach. Rather than having a single statute and regulator dealing with privacy matters, there is a patchwork of different legislation with a multiplicity of regulators with overlapping jurisdictions. Due to the lack of a comprehensive primary federal information privacy statute, e-commerce users and the private sector face a confusing regulatory regime at the federal level.5

There is for example a different statutory regime that applies to the protection of privacy involving the telecommunications industry and e-marketing is covered by separate legislation under the telecommunications legislation and the Spam Act. Besides the Australian Information Commissioner who is responsible for privacy codes, there is the ACMA and the Telecommunications industry Ombudsman (TIO) involved in approving industry codes of practice in the telecommunications sector. The inconsistencies between the coverage of telecommunications legislation and the Privacy Act 1988 (Cth) require at the very minimum consistent definitions and consistent levels of protection and enforcement. The current approach whereby separate legislation applies to particular

---

5 See ‘Information Technology: As Data Privacy Laws Evolve Globally, Many Nations Consider European Model’, *BNA’s International Trade Reporter, Analysis & Perspective* (1 May 2003), cited in Wakako Takatori, ‘Cross-border Trade of Personal Data: Impact of Privacy Laws on the Private Sector and Analysis under GATS Framework’. The personal information collected by financial institutions is covered by the Financial Services Modernisation (Gramm-Leach-Bliley) Act 1999(U.S.), while the personal information of children collected and processed online is protected under the *Children’s Online Privacy Protection Act* (COPPA) 1998 (U.S.).
sectors (such as telecommunications) or problems (such as spam email) does not provide a coherent response to privacy protection. For example, small businesses are exempted from the Privacy Act but are subject to the privacy protection provisions of the telecommunications legislation; and the Privacy Act does not regulate spam but the Spam Act does. These problems can be avoided by a single federal statute covering privacy.  

9.6.2 The Privacy Act - the Human Right of Privacy

Unlike the European approach, the Australian legislation gives preference to commercial efficiency over and above rights to the personal privacy of e-commerce users. Indicative are the exemptions for small businesses, and the provision for disclosure and use of personal information by third parties without consent particularly in relation to e-marketing and transfer to related businesses. It is this preference of commercial interests over privacy that restricts the protection given to the e-commerce user and allows commercial interests to trump human rights to privacy. The Australian position should be aligned with the approach taken by the EU that is interferences with privacy are only permitted where there is a compelling case requiring interference; commercial interests and efficiency do not suffice.

9.6.3 Privacy Protection - the Changing Technology Environment

The principal Australian legislation, the Privacy Act was enacted in 1988 when e-commerce was in its infancy. Although the legislation was intended to be technologically neutral and adaptable in times of rapid technological change, the reality is that it has not kept pace with developments. Its provisions predate the development of data mining and the various forms of behavioural analysis alluded to in chapter 2. It has not kept up with the capacity of the internet to invade e-commerce users’ personal privacy. The Privacy Act 1988 (Cth) does not specifically cover the activities of ISPs although these are covered

---


7 The ALRC has recommended removing or modifying a number of exemptions to the Privacy Act for small business, employees and political parties. For further details refer to Australian Law Reform Commission, ‘For Your Information: Australian Privacy Law and Practice’ (Report 108); Small businesses (see [39.181]-[39.191], Recommendation 39-1); Employee records (see - [40.121]-[40.122], Recommendations 40-1, 40-2); Political parties (see [41.90]-[41.91], Recommendation 41-4).
under the telecommunications and spam legislation. Unlike the developments in the European Union referred to in chapter 5, the Australian legislation has not expanded to include processors or those who make decisions about data both of whom are subject to responsibilities under the European Commission Directives. Consequently the Australian privacy protection framework is patchy rather than comprehensive.

9.6.4 Privacy Protection under Industry Regulation

Besides statutory regulation, industry regulation has played a role in privacy protection in Australia. The current industry based approach to privacy also fails to provide a coherent approach to the protection of privacy for the e-commerce user. There is for example multiplicity of regulators in the development, approval, enforcement of industry codes and different outcomes for complainants depending on to whom the complaint is lodged with. It has also been observed in chapter 8, that the industry has not taken up opportunities the under the Privacy Act to develop industry based privacy codes.

Industry regulators and their role and powers were discussed in chapter 7. ACMA is responsible for the enforcement of the Telecommunication (Interception) Act 1997 (Cth); Telecommunications Act 1997 (Cth), the Spam Act 2003 (Cth), the Do Not Call Register Act 2006 (DNCR Act) all of which deal with privacy matters. If a special level of industry expertise is required to deal with these matters, there is no reason why this type of expertise could not be embedded within a single privacy body or Commission that gives the e-commerce user a single avenue to complain, have issues investigated and obtain uniform remedies under a single regulator.

The impact and effectiveness of industry regulation was discussed in chapter 8. There are industry specific codes under telecommunications legislation and codes implementing the Spam Act. It is also apparent that industry regulation for example in the form of the TCP Code and the e-Marketing Code that were examined in chapter 8, provides a much more efficient and timely mechanisms for dispute resolution. Although there is value in industry expertise in recognising and responding to privacy issues within a particular sector, there are significant barriers to the effective protection of an e-commerce users’ personal information.
In respect to the two industry codes examined in chapter 8, that is the TCP Code and the e-Marketing Code, in comparison to the NPPs, there is disparity in the level of complaints handling, compliance, enforcement and outcomes for individuals when their privacy has been breached by organisations that are bound by the TCP Code and the e-Marketing code. The disparity between the telecommunications legislation and the Privacy Act has created a lack of understanding of the law that contributes to the noncompliance. A single set of mandatory information protection principles would lead to a clearer understanding of obligations and reduce the disparity between the Privacy Act and the telecommunications legislation.

9.7 What More Needs to Be Done

The following sections examine how privacy laws in Australia can be harmonised and law reform initiatives as possible measures for better privacy protection.

9.7.1 Law Reform Initiatives

Australia is currently in the process of reviewing its existing domestic frameworks as will be discussed in the sections following. The first issue is the provision of a single regulator operating under a single legislative regime.

9.7.1.1 Australian Federal Statutory Privacy Protection

The Australian legal framework and privacy laws need to provide more adequate and effective personal information privacy protection for e-commerce users.\textsuperscript{8} Firstly, in order to avoid inconsistencies and gaps in protection, there should be a single regulator and a single piece of legislation regulating privacy rather than the current multiplicity of regulators with overlapping jurisdiction as well as different legislative regimes under telecommunications legislation and spam legislation referred to in chapter 6. The ALRC has made recommendations in respect to a uniform set of privacy principles that will be applicable in relation to collection, use and disclosure of personal information, access and correction and the transborder flows of personal information.

Secondly, the reach of the legislation should extend to the changing technology with broader definitions of what is ‘personal information’, and an extended definition of those who are subject to privacy obligations. The broader definitions used in the EU directive imposing duties on data controllers and processors should be adopted (see chapter 5 [5.3.2.1]; [5.3.2.2]). The ALRC has highlighted in its review of the Australian privacy protection framework,\(^9\) the inadequacy of making incremental amendments to outdated legislation in an attempt to deal with modern technology. The ALRC has recommended that legislation be introduced to respond to the ongoing technological developments and the consequent policy implications.\(^10\)

Thirdly, currently, the Privacy Act does not provide strong incentives for organisations to comply with the NPPs. The core privacy protection principles NPPs, subject to recommended amendments, should be mandatory for those who process (that is collect, use and disclose) or make decisions about personal information without exceptions.

Fourthly, as a measure to give greater assurance to the protection of e-commerce users’ privacy, there should be implemented a requirement of prior registration and notification to the supervisory body about the collection, use and disclosure of personal information. There should be the additional requirement of express consent in which constraints on decision making by the e-commerce user are minimised. That is, the e-commerce user must be put in control of their personal information by providing easily accessible information in language suitable for the average user about the collection, usage and disclosure of that personal information. Where possible the e-commerce user should be given a genuine opportunity to decide whether to agree to the collection, usage and disclosure of their personal information.

Fifthly, the new privacy regulator should be given a much stronger compliance, monitoring, investigatory and enforcement regime such as exists under the Telecommunications and Spam Acts. A stronger compliance regime which replicated the stronger powers available under the Telecommunications and Spam Acts to impose civil

---

9 Australian Law Reform Commission, above n 7.
penalties for serious or repeated breaches of the Privacy Act should be implemented. Only then will e-commerce users’ right to privacy receive adequate protection.

9.8 Conclusion

This thesis has examined the current framework for privacy protection in Australian; how it got there; and what more needs to be done for effective information privacy protection for e-commerce users in Australia.

Privacy and trust are important aspects of e-commerce. In line with the ALRC’s recommendations discussed above, it is recommended that, at the federal level, there be a single regulator operating under an amended Privacy Act that covers information privacy with a single set of unified privacy principles that apply to all data collectors in all sectors. This measure will allow for more effective, easier to implement, easier to monitor and enforce compliance and create less confusion about which legislation or code applies.

The law alone will not adequately protect privacy and foster confidence in the digital economy and the online environment. Information privacy will be better protected by adopting a multi-faced approach when legislation such as the Privacy Act is combined with end user empowerment through education and awareness so that e-commerce users are capable of managing privacy invasive technologies. Embedding privacy protection by design of networked information and communication technology (ICT) systems will enhance trust amongst e-commerce users and organisations. Privacy protection in Australia can also be enhanced through: a) harmonization of laws; b) accountability; c) openness and transparency in data collection; d) data security (risk assessment and management of digital data initiatives in place by the regulators and the industry as one of the solutions in overcoming the problem of information privacy protection); e) creating greater awareness of information privacy issues and protection; and f) co-operation within national and international regulators.

This was also recommended by the ALRC. See Australian Law Reform Commission, above n 9, [50.35]-[50.55], Recommendations 50-2, 50-3, 50-4.
Bibliography

1. Books


American Law Institute, Restatement (Second) of Torts § 652 (American Law Institute, 1977).

Ang, Peng Hwa, Ordering Chaos: Regulating the Internet (Delmar, 2005).


Biegel, Stuart, Beyond our Control? Confronting the limits of our legal systems in the age of Cyberspace (MIT Press, 2001).

Cate, Fred H, Privacy in the Information Age (Brookings Institution, 1st ed, 1997).

Chander, Anupam, Lauren Gelman and Margaret Jane Radin, Securing Privacy in the Internet Age (Stanford University Press, 2005).


Feinberg, Joel and Hyman Gross (eds), Philosophy of law (Wadsworth Publishing Company, 1986).


Finnis, John, Natural Law and Natural Right (Clarendon Press, 1980).

Flaherty, David H, Privacy and Data Protection: An International Bibliography (Mansell, 1984).


Henderson, Harry, Privacy in the information age (Facts On File, 1999).


Mappes, Thomas A, & David DeGazia,, Biomedical Ethics (Mcgraw-Hill College, 4th ed, 1995)


O'Harrow, Robert Jr, No Place to Hide (Free Press, 2005).

Price, Monroe E and Stefan G Verhulst (eds), In search of the self: charting the course of self-regulation on the Internet in a global environment, Regulating the Global Information Society (Routledge, 2000).


Schneider, Gary P, Electronic Commerce (Cengage Learning, 9 ed, 2010).

Schneier, Bruce, Secrets and lies: Digital security in the network world (John Wiley & Sons, 2000).


Simmonds, Nigel E, Central Issues in Jurisprudence: Justice, Law and Rights (Sweet & Maxwell, 1986).


Tyree, Alan L, Banking Law in Australia (Butterworths, 2nd ed, 1995).

Tyree, Alan L, Digital Cash (Butterworths, 1st ed, 1997).


2. Journal Articles


Clarke, Roger, 'Information Technology and Dataveillance' (1988) 31(5) Communications of the ACM.


Fried, Charles, 'Privacy' (1968) 77 Yale Law Journal 75.


Gerstein, Robert S, 'Intimacy and Privacy' (1978) 89 Ethics 76.


Phillips, David J, 'Privacy Policy and PETs: The influence of policy regimes on the
development and social implications of privacy enhancing technologies' (2004) 6(6) New
Media and Society 15.

Phillips, David J, 'Negotiating the Digital Closet: Online Pseudonymity and the Politics of

Rajaretnam, Thilla, ‘The Problem to Consent to the Collection, Use, and Disclosure of
Personal Information in Cyberspace’ (2012) International Journal of Cyber-Security and
Digital Forensics (IJCSD) 1(3) 241-247; The Society of Digital Information and Wireless
Communications (SDIWC) Nov. 2012 (ISSN: 2305-0012).

Rajaretnam, Thilla, ‘The Right to Consent and Control Personal Information Processing in
(IJCSD) 1(3) 232-240; The Society of Digital Information and Wireless Communications
(SDIWC) Nov. 2012 (ISSN: 2305-0012).

Reidenberg, Joel R, 'Privacy in the Information Economy: A Fortress or Frontier for

Reidenberg, Joel R, 'Resolving Conflicting International Data Privacy Rules in

Robertson, Steven, 'Offshore Business Processing in China Brings Privacy Concerns'

74(3) Indiana Law Journal 893.

Sainty, Katherine and Andrew Ailwood, 'Implications of Transborder Data Flow for

Schwartz, Paul M and Karl-Nikolaus Piefer, 'Prosser’s Privacy and the German Right of
Personality: Are Four Privacy Torts Better than One Unitary Concept?' (2010) 98
California Law Review 63.


3. Reports/Discussion Papers/Consultations


Australian Communications and Media Authority, Annual Report: 1 July 2008-30 June 2009 (Australian Communications and Media Authority, 2009).

Australian Communications and Media Authority, Annual Report: 1 July 2009-30 June 2010 (Australian Communications and Media Authority, 2010).

Australian Communications and Media Authority, Annual Report: 1 July 2010-30 June 2011 (Australian Communications and Media Authority, 2011).

Australian Communications and Media Authority, Australian E–marketing Code of Practice (Australian Communications and Media Authority, 2005).

Australian Communications and Media Authority, Complaints, Reports and Enquiries (Australian Communications and Media Authority, 2011).
Australian Communications and Media Authority, Compliance and Enforcement Bulletin (Australian Communications and Media Authority, 2011).

Australian Communications and Media Authority, Do Not Call Register (Australian Communications and Media Authority, 2011).

Australian Communications and Media Authority, Reconnecting the Customer (Australian Communications and Media Authority, 2011).


Australian Direct Marketing Association (ADMA), Interim Review of the ADMA Code (Australian Direct Marketing Association, 7 July 2011)


Australian Direct Marketing Association (ADMA), Direct Marketing Code of Practice (Australian Direct Marketing Association, 2006).


Cyberspace Law and Policy Centre, University of New South Wales(UNSW), Submission PR 487 to the Australian Law Reform Commission on Data Security, Disclosure of Personal Information to Third Parties(Cyberspace Law and Policy Centre, UNSW, 19 December 2007).


Environment and Communications Reference Committee, Senate, Parliament of Australia, The adequacy of protection for privacy of Australians Online (Canberra, 7 April 2011).


Office of the Australian Information Commissioner, Privacy Law Reform: Challenges and Opportunities (Office of the Australian Information Commissioner, 23 February 2012).

Office of the Australian Information Commissioner (OAIC), 'Own Motion Investigation Report - Vodafone Hutchinson Australia’ (Office of the Australian Information Commissioner 2011).


Office of the Privacy Commissioner, Community Attitudes to Privacy (Office of the Privacy Commissioner, 2007).


Office of the Privacy Commissioner, Guide to handling personal information security breaches (Office of the Privacy Commissioner, 2008).

Office of the Privacy Commissioner, Guidelines to the National Privacy Principles (Office of the Privacy Commissioner, 2001).


Privacy New South Wales (Privacy NSW), Submission on the Review of the Privacy and Information Protection Act 1988 (PIPA) (Privacy NSW, 2004).

Select Committee on Information Technologies, Senate, Parliament of Australia, Cookie Monsters? Privacy in the information society (Canberra, November 2000).


Tasman Asia Pacific Economic, Management and Policy Consultants, Analysis of market circumstances where industry self-regulation is likely to be most and least effective (Tasman Asia Pacific Economic, Management and Policy Consultants, 2000) (prepared by John Wallace, Denise Ironfield and Jennifer Orr).


Data Protection Supervisor (‘EDPS’), Executive summary, EDPS Opinion of 7 March 2012 on the data protection reform package (2012/C 192/05) (Data Protection Supervisor (‘EDPS’), 7 March 2012).

4. List of Legislation

Acts Interpretation Act 1901(Cth).


Archives Act 1983 (Cth).

Australian Constitution Act 1901 (Cth).

California Online Privacy Protection Act of 2003 (U.S.).


Civil Law (Wrongs) Act 2002 (ACT).

Competition and Consumer Act 2010 (Cth).

Competition and Consumer Act 2010 (Cth) sch 2 Australian Consumer Law (No.1) 2010 (Cth).

Competition and Consumer Act 2010 (Cth) sch 2 Australian Consumer Law Act (No.2) 2010 (Cth).
Consumer Affairs and Fair Trading Act 1990 (NT).

Corporations Act 2001 (Cth).

Crimes Act 1914 (Cth).

Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Act (No.2) 2004 (Cth).


Data Protection Act 1993 (UK).

Do Not Call Register Act 2006 (Cth).

Electronic Transaction Act 1999 (Cth).

Fair Trading Act 1987 (NSW).

Fair Trading Act 2010 (WA).

Financial Services Modernisation (Gramm-Leach-Bliley) Act 1999 (U.S.).

Insurance Contracts Act 1984 (Cth).

Misrepresentation Act 1972 (SA).

Online Privacy Protection Act of 2003 (U.S.).

Privacy Act 1988 (Cth).

Privacy Act 1993 (NZ).

Privacy Act 1974 (U.S.).

Privacy Amendment (Private sector) Act 2001 (Cth).

Privacy and Personal Information Protection Act 1998 (NSW).

Spam Act 2003 (Cth).
Telecommunications (Consumer Protection and Service Standards) Act 1999 (Cth).

Telecommunications Act 1997 (Cth).


5. List of Case Law


Bromley v Ryan (1956) 99 CLR 362.


Victoria Park Racing and Recreation Grounds Co Ltd v Taylor (1937) 58 CLR 479.

Williams v Settle (1960) 1 WLR 1072.

6. List of Administrative Decisions by the Australian Information Commissioner (OAIC)


Own Motion Investigation Report - Own Motion Investigation v Information Technology Company [2010] PrivCmrA 24 ' (Australian Information Commissioner (OAIC), 2010).

Own Motion Investigation v Telecommunications Company [2010] PrivCmrA 16' (Australian Information Commissioner (OAIC), 2010).

7. International treaties and conventions, reports, and discussion papers


European Commission, Proposals for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data

International Covenant on Economic, Social and Cultural Rights (ICESCR), adopted and open for signature, ratification and accession by United Nations General Assembly resolution 2200A (XXI) of the 16 December 1966 (entry into force 3 January 1976), in accordance with Article 27.

International Covenant on Civil and Political Rights (ICCPR), adopted and opened for signature, ratification and accession by General Assembly resolution 2200A (XXI) of 16 December 1966 (entry into force 23 March 1976) in accordance with Article 49 (“ICCPR 1976”).


8. Other Sources

ABC News, Facebook admits privacy breach (online) (19 October 2010)


Australian Communications Consumer Action Network (ACCAN), Major Telstra privacy breach affects 220,000 customers – OPC must act, Media Release (27 October 2010).


232


233
Clarke, Roger, The Effectiveness of Privacy Policy Statements (2008)  


Stepanek, Marcia, Weblining: Companies are using your personal data to limit your choices--and force you to pay more for products, Businessweek (online) (3 April 2000) <http://www.businessweek.com/2000/00_14/b3675027.htm>.


Walters, Conrad, Consumers have a right to be told of the dangers, The Sydney Morning Herald, (Sydney) (8 April 2011).


Appendix 1: OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

PREFACE¹

The development of automatic data processing, which enables vast quantities of data to be transmitted within seconds across national frontiers, and indeed across continents, has made it necessary to consider privacy protection in relation to personal data. Privacy protection laws have been introduced, or will be introduced shortly, in approximately one half of OECD Member countries (Austria, Canada, Denmark, France, Germany, Luxembourg, Norway, Sweden and the United States have passed legislation. Belgium, Iceland, the Netherlands, Spain and Switzerland have prepared draft bills) to prevent what are considered to be violations of fundamental human rights, such as the unlawful storage of personal data, the storage of inaccurate personal data, or the abuse or unauthorised disclosure of such data.

On the other hand, there is a danger that disparities in national legislations could hamper the free flow of personal data across frontiers; these flows have greatly increased in recent years and are bound to grow further with the widespread introduction of new computer and communications technology. Restrictions on these flows could cause serious disruption in important sectors of the economy, such as banking and insurance.

For this reason OECD Member countries considered it necessary to develop Guidelines which would help to harmonise national privacy legislation and, while upholding such human rights, would at the same time prevent interruptions in international flows of data. They represent a consensus on basic principles which can be built into existing national legislation, or serve as a basis for legislation in those countries which do not yet have it.

The Guidelines, in the form of a Recommendation by the Council of the OECD, were developed by a group of government experts under the chairmanship of the Hon. Justice Michael Kirby, Chairman of the Australian Law Reform Commission. The Recommendation was adopted and became applicable on 23rd September, 1980.

The Guidelines are accompanied by an Explanatory Memorandum intended to provide information on the discussion and reasoning underlining their formulation.

¹ This is an unofficial text. For the authoritative text of the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, reference should be made to the OECD’s web site. The OECD Guidelines are available at <http://ww.oecd.org/documentprint/0,3455,en_2649_34255_1815186_1_1_1_1,00.html>.
RECOMMENDATION OF THE COUNCIL CONCERNING GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (23rd September, 1980)

THE COUNCIL,

Having regard to articles 1(c), 3(a) and 5(b) of the Convention on the Organisation for Economic Co-operation and Development of 14th December 1960;

RECOGNISING:

- that, although national laws and policies may differ, Member countries have a common interest in protecting privacy and individual liberties, and in reconciling fundamental but competing values such as privacy and the free flow of information;
- that automatic processing and transborder flows of personal data create new forms of relationships among countries and require the development of compatible rules and practices;
- that transborder flows of personal data contribute to economic and social development;
- that domestic legislation concerning privacy protection and transborder flows of personal data may hinder such transborder flows;

Determined to advance the free flow of information between Member countries and to avoid the creation of unjustified obstacles to the development of economic and social relations among Member countries;

RECOMMENDS:

1. That Member countries take into account in their domestic legislation the principles concerning the protection of privacy and individual liberties set forth in the Guidelines contained in the Annex to this Recommendation which is an integral part thereof;

2. That Member countries endeavour to remove or avoid creating, in the name of privacy protection, unjustified obstacles to transborder flows of personal data;

3. That Member countries co-operate in the implementation of the Guidelines set forth in the Annex;

4. That Member countries agree as soon as possible on specific procedures of consultation and co-operation for the application of these Guidelines.

Annex to the Recommendation of the Council of 23rd September 1980
GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND
TRANSBORDER FLOWS OF PERSONAL DATA

PART ONE. GENERAL

Definitions

1. For the purposes of these Guidelines:

a) ‘data controller’ means a party who, according to domestic law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf:

b) ‘personal data’ means any information relating to an identified or identifiable individual (data subject);

c) ‘transborder flows of personal data’ means movements of personal data across national borders.

Scope of Guidelines

2. These Guidelines apply to personal data, whether in the public or private sectors, which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a danger to privacy and individual liberties.

3. These Guidelines should not be interpreted as preventing:

a) the application, to different categories of personal data, of different protective measures depending upon their nature and the context in which they are collected, stored, processed or disseminated;

b) the exclusion from the application of the Guidelines of personal data which obviously do not contain any risk to privacy and individual liberties; or

c) the application of the Guidelines only to automatic processing of personal data.

4. Exceptions to the Principles contained in Parts Two and Three of these Guidelines, including those relating to national sovereignty, national security and public policy (‘order public’), should be:

a) as few as possible, and

b) made known to the public.
5. In the particular case of Federal countries the observance of these Guidelines may be affected by the division of powers in the Federation.

6. These Guidelines should be regarded as minimum standards which are capable of being supplemented by additional measures for the protection of privacy and individual liberties.

PART TWO. BASIC PRINCIPLES OF NATIONAL APPLICATION

Collection Limitation Principle

7. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Data Quality Principle

8. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up to-date.

Purpose Specification Principle

9. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation Principle

10. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:

a) with the consent of the data subject; or

b) by the authority of law.

Security Safeguards Principle

11. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

Openness Principle

12. There should be a general policy of openness about developments, practices and
policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

**Individual Participation Principle**

13. An individual should have the right:

**Appendix 7 193**

a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;

b) to have communicated to him, data relating to him

☐ within a reasonable time;

☐ at a charge, if any, that is not excessive;

☐ in a reasonable manner; and

☐ in a form that is readily intelligible to him;

c) to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and

d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

**Accountability Principle**

14. A data controller should be accountable for complying with measures which give effect to the principles stated above.

**PART THREE. BASIC PRINCIPLES OF INTERNATIONAL APPLICATION:**

**FREE FLOW AND LEGITIMATE RESTRICTIONS**

15. Member countries should take into consideration the implications for other Member countries of domestic processing and re-export of personal data.

16. Member countries should take all reasonable and appropriate steps to ensure that transborder flows of personal data, including transit through a Member country, are uninterrupted and secure.
17. A Member country should refrain from restricting transborder flows of personal data between itself and another Member country except where the latter does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation. A Member country may also impose restrictions in respect of certain categories of personal data for which its domestic privacy legislation includes specific regulations in view of the nature of those data and for which the other Member country provides no equivalent protection.

18. Member countries should avoid developing laws, policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to transborder flows of personal data that would exceed requirements for such protection.

**PART FOUR. NATIONAL IMPLEMENTATION**

19. In implementing domestically the principles set forth in Parts Two and Three, Member countries should establish legal, administrative or other procedures or institutions for the protection of privacy and individual liberties in respect of personal data. Member countries should in particular endeavour to:

a) adopt appropriate domestic legislation;

b) encourage and support self-regulation, whether in the form of codes of conduct or otherwise;

c) provide for reasonable means for individuals to exercise their rights;

d) provide for adequate sanctions and remedies in case of failures to comply with measures which implement the principles set forth in Parts Two and Three;

e) ensure that there is no unfair discrimination against data subjects.

**PART FIVE. INTERNATIONAL CO-OPERATION**

20. Member countries should, where requested, make known to other Member countries details of the observance of the principles set forth in these Guidelines.

Member countries should also ensure that procedures for transborder flows of personal data and for the protection of privacy and individual liberties are simple and compatible with those of other Member countries which comply with these Guidelines.

21. Member countries should establish procedures to facilitate:

- information exchange related to these Guidelines, and
□ mutual assistance in the procedural and investigative matters involved.

22. Member countries should work towards the development of principles, domestic and international, to govern the applicable law in the case of transborder flows of personal data.
Appendix 2: European Union Directives on Information Protection

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

CHAPTER 1

GENERAL PROVISIONS

Article 1

Object of the Directive

1. In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons and in particular their right to privacy, with respect to the processing of personal data.

2. Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1.

Article 2 Definitions

For the purposes of this Directive:

(a) personal data shall mean any information relating to an identified or identifiable natural person (data subject); an identifi able person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

(b) processing of personal data (processing) shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

(c) personal data filing system (filing system) shall mean any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;

(d) controller shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data. Where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by a national or Community law.

(e) processor shall mean the natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;

(f) third party shall mean the natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data;

(g) recipient shall mean the natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients;

(h) the data subject’s consent shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.

Article 3 Scope

1. This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.

2. This Directive shall not apply to the processing of personal data:

   o in the course of an activity which falls outside the scope of community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation is bound up with questions of State security) and the activities of the State in areas of criminal law;
   o by a natural person in the course of a purely personal or household activity.

Article 4 National law applicable

1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:
(a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;

(b) the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law;

(c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.

2. In the circumstances referred to in paragraph 1(c), the controller must designate a representative established in the territory of that Member State, without prejudice to legal actions which could be initiated against the controller himself.

CHAPTER II

GENERAL RULES ON THE LAWFULNESS OF THE PROCESSING OF PERSONAL DATA

Article 5

Member States shall, within the limits of the provisions of this Chapter, determine more precisely the conditions under which the processing of personal data is lawful.

SECTION 1

PRINCIPLES RELATING TO DATA QUALITY

Article 6

1. Member States shall provide that personal data must be:

(a) processed fairly and lawfully;

(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;
(c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or for which they are further processed;

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;

(e) kept in a form which permits identification of data subjects for no longer that is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.

2. It shall be for the controller to ensure that paragraph 1 is complied with.

SECTION II

PRINCIPLES RELATING TO THE REASONS FOR MAKING DATA PROCESSING LEGITIMATE

Article 7

Member States shall provide that personal data may be processed only if:

(a) the data subject has given his consent unambiguously; or

(b) processing is necessary for the performance of a contact to which the data subject is party or in order to take steps at the request of the data subject entering into a contract; or

(c) processing is necessary for compliance with a legal obligation to which the controller is subject; or

(d) processing is necessary in order to protect the vital interests of the data subject; or

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection under Article 1(1).
SECTION III

SPECIAL CATEGORIES OF PROCESSING

Article 8 The processing of special categories of data

1. Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

2. Paragraph 1 shall not apply where:

(a) the data subject has given his explicit consent to the processing of those data, except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be waived by the data subject giving his consent.; or

(b) processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law insofar as it is authorized by national law providing for adequate safeguards; or

(c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or

(d) processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects; or

(e) the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims.

3. Paragraph 1 shall not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

4. Subject to the provision of suitable safeguards, Member States may lay down for reasons of important public interest, exemptions in addition to those laid down in paragraph 2 either by national law or by decision of the supervisory authority.
5. Processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law, subject to derogations which may be granted by the Member State under national provisions providing suitable specific safeguards. However, a complete register of criminal convictions may be kept only under the control of official authority.

Member States may provide that data relating to administrative sanctions or civil trials shall also be processed under the control of official authority.

6. Derogations from paragraph 1 provided for in paragraphs 4 and 5 shall be notified to the Commission.

7. Member States shall determine the conditions under which a national identification number or any other identifier of general application may be processed.

**Article 9 Processing of personal data and freedom of expression**

Member States shall provide for exemptions or derogations from the provisions of this Chapter, Chapter IV and Chapter VI for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.

**SECTION IV**

**INFORMATION TO BE GIVEN TO THE DATA SUBJECT**

**Article 10 Information in cases of collection of data from the data subject**

Member States shall provide that the controller or his representative must provide a data subject from whom data relating to himself are collected with at least the following information, except where he already knows:

(a) the identity of the controller and of his representative, if any,

(b) the purposes of the processing for which the data are intended,

(c) any further information such as

- the recipients or categories of recipients of the data;
- whether replies to the questions are obligatory or voluntary, as well as the possible consequences of the failure to reply;
Article 11 Information where the data have not been obtained from the data subject

1. Where the data have not been obtained from the data subject, Member States shall provide that the controller or his representative must at the time of undertaking the recording of personal data or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed provide the data subject with at least the following information, except where he already knows:

(a) the identity of the controller and of his representative, if any,
(b) the purposes of the processing,
(c) any further information such as
   - the categories of data concerned
   - the recipients or categories of recipients;
   - the existence of the right of access to and the right to rectify the data concerning him insofar as they are necessary, having regard to the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject.

2. Paragraph 1 shall not apply where, in particular for processing for statistical purposes or for the purposes of historical or scientific research, the provision of information proves impossible or involves a disproportionate effort or if recording or disclosure is expressly laid down by law. In these cases Member States shall provide appropriate safeguards.

SECTION V

THE DATA SUBJECT'S RIGHT OF ACCESS TO DATA

Article 12 Right of access

Member States shall guarantee for every data subject the right to obtain from the controller:

1. without constraint at reasonable intervals and without excessive delay or expense:
   - confirmation as to whether or not data relating to him are processed and information
   - at least as to the purposes of the processing, the categories of data concerned, and the
   - recipients or categories of recipients to whom the data are disclosed;
   - communication to him in an intelligible form of the data undergoing processing and
   - of any available information as to their source;
knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15(1);

2. as appropriate the rectification, erasure or blocking of data, the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;

3. notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with paragraph 2, unless this proves impossible or involves a disproportionate effort.

SECTION VI

EXEMPTIONS AND RESTRICTIONS

Article 13 Exemptions and restrictions

1. Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6(1), 10, 11(1), 12 and 21 when such a restriction constitutes a necessary measure to safeguard:

(a) national security;

(b) defence;

(c) public security;

(d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;

(e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;

(f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);

(g) the protection of the data subject or of the rights and freedoms of others.

2. Subject to adequate legal guarantees, in particular that the data are not used for taking measures or decisions regarding any particular individual data subject, Member States may restrict, by a legislative measure, the rights provided for in Article 12 when data are processed solely for purposes of scientific research or are kept in personal form for a period which does not exceed the period necessary for the sole purpose of creating statistics.
SECTION VII

THE DATA SUBJECT'S RIGHT TO OBJECT

Article 14 The data subject's right to object

Member States shall grant the data subject the right:

(a) at least in the cases referred to in Article 7(e) and (f), to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data;

(b) to object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing; or

...to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses.

Member States shall take the necessary measures to ensure that data subjects are aware of the existence of the right referred to in the first subparagraph of (b).

Article 15 Automated individual decisions

1. Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.

2. Subject to the other Articles of this Directive, Member States shall provide that a person may be subjected to a decision of the kind referred to in paragraph 1 if that decision:

(a) is taken in the course of entering into or performance of a contract, provided the request by the data subject has been satisfied, or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to defend his point of view; or

(b) is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests.
SECTION VIII

CONFIDENTIALITY AND SECURITY OF PROCESSING

Article 16 Confidentiality of processing

Any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data, must not process them except on instructions from the controller, unless he is required to do so by law.

Article 17 Security of processing

1. Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss and against unauthorized alteration, disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Having regard to the state of the art and the costs of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

2. The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor who provides sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out and must ensure compliance with those measures.

3. The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that:

- the processor shall act only on instructions from the controller;
- the obligations set out in paragraph 1, as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor.

4. For the purposes of keeping proof, the parts of the contract or legal act relating to data protection and the requirements relating to the measures referred to in paragraph 1 shall be in writing or in another equivalent form.
SECTION IX

NOTIFICATION

Article 18 Obligation to notify the supervisory authority

1. Member States shall provide that the controller or his representative, if any, must notify the supervisory authority referred to in Article 28 before carrying out any wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes.

2. Member States may provide for the simplification of or exemption from notification only in the following cases and under the following conditions:

- where, for categories of processing operations which are unlikely, taking account of the data to be processed, to affect adversely the rights and freedoms of data subjects, they specify the purposes of the processing, the data or categories of data undergoing processing, the category or categories of data subject, the recipients or categories of recipient to whom the data are to be disclosed and the length of time the data are to be stored and/or

  o where the controller appoints, in compliance with the national law which governs him, a data protection official, responsible in particular
  o for ensuring in an independent manner the internal application of the national provisions taken pursuant to this Directive
  o for keeping the register of processing operations carried out by the controller, containing the items of information referred to in Article 21(2), thereby ensuring that the rights and freedoms of the data subjects are unlikely to be adversely affected by the processing operations.

3. Member States may provide that paragraph 1 does not apply to processing whose sole purpose is the keeping of a register, which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person demonstrating a legitimate interest.

4. Member States may provide for an exemption from the obligation to notify or a simplification of the notification in the case or processing operations referred to in Article 8(2) (d).

5. Member States may stipulate that certain or all non-automatic processing operations involving personal data shall be notified, or provide for these processing operations to be subject to a simplified notification.
Article 19 Contents of notification

1. Member States shall specify the information to be given in the notification. It shall include at least:

(a) the name and address of the controller and of his representative, if any;

(b) the purpose or purposes of the processing;

(c) a description of the category or categories of data subject and of the data or categories of data relating to them;

(d) the recipients or categories of recipient to whom the data might be disclosed;

(e) proposed transfers of data to third countries;

(f) a general description allowing a preliminary assessment to be made of the appropriateness of the measures taken pursuant to Article 17 to ensure security of processing.

2. Member States shall specify the procedures under which any change affecting the information referred to in paragraph 1 must be notified to the supervisory authority.

Article 20 Prior checking

1. Member States shall determine the processing operations likely to present specific risks for the rights and freedoms of data subjects and shall check that these processing operations are examined prior to the start thereof.

2. Such prior checks shall be carried out by the supervisory authority following receipt of a notification from the controller or by the data protection official, who in cases of doubt must consult the supervisory authority.

3. Member States may also carry out such checks in the context of preparation of a measure decided on by the national parliament or based on such a decision, defining the nature of the processing operation and laying down appropriate safeguards.

Article 21 Publicizing of processing operations

1. Member States shall take measures to ensure that processing operations are publicized.

2. Member States shall provide that a register of processing operations notified in accordance with Article 18 shall be kept by the supervisory authority.

The register shall contain at least the information listed in Article 19(1) (a) to (e).
The register may be inspected by any person.

3. Member States shall provide, in relation to processing operations not subject to notification, that controllers or another body appointed by the Member States make available at least the information referred to in Article 19(1) (a) to (e) in an appropriate fashion to any person on request.

Member States may provide that this provision does not apply to processing whose sole purpose is the keeping of a register, which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can provide proof of a legitimate interest.

CHAPTER III

JUDICIAL REMEDIES, LIABILITY AND PENALTIES

Article 22 Remedies

Without prejudice to any administrative remedy for which provision may be made, inter alia before the supervisory authority referred to in Article 28, prior to referral to the judicial authority, Member States shall provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing in question.

Article 23 Liability

1. Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered.

2. The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage.

Article 24 Sanctions

The Member States shall adopt suitable measures to ensure the full implementation of the provisions of this Directive and shall in particular lay down the sanctions to be imposed in case of infringement of the provisions adopted pursuant to this Directive.
CHAPTER IV

TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES

Article 25 Principles

1. Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.

2. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in those countries.

3. Member States and the Commission shall inform each other of cases where they consider that a third country does not ensure an adequate level of protection within the meaning of paragraph 2.

4. Where the Commission finds, under the procedure provided for in Article 31(2), that a third country does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article Member States shall take the measures necessary to prevent the transfer of data of the same type to the third country in question.

5. At the appropriate time, the Commission shall enter into negotiations with a view to remedying the situation resulting from the funding made pursuant to paragraph 4.

6. The Commission may find, in accordance with the procedure referred to in Article 31(2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals.

Member States shall take the measures necessary to comply with the Commission's decision.
Article 26 Derogations

1. By way of derogation from Article 25 and save where otherwise provided by domestic law governing particular cases, Member States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25(2) may take place on condition that:

1) the data subject has given his consent unambiguously to the proposed transfer, or

2) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken in response to the data subject's request, or

3) the transfer is necessary for the conclusion or for the performance of a contract concluded in the interest of the data subject between the controller and a third party, or

4) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims, or

5) the transfer is necessary in order to protect the vital interests of the data subject, or

6) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

2. Without prejudice to paragraph 1, a Member State may authorize a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25(2), where the controller adduces sufficient guarantees with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such guarantees may in particular result from appropriate contractual clauses.

3. The Member State shall inform the Commission and the other Member States of the authorizations granted pursuant to paragraph 2.

If a Member State or the Commission objects on justified grounds involving the protection of the privacy and fundamental rights and freedoms of individuals, the Commission shall take appropriate measures in accordance with the procedure laid down in Article 31(2).

Member States shall take the necessary measures to comply with the Commission's decision.
4. Where the Commission decides, in accordance with the procedure referred to in Article 31(2), that certain standard contractual clauses offer sufficient guarantees required by paragraph 2, Member States shall take the necessary measures to comply with the Commission's decision.

CHAPTER V

CODES OF CONDUCT

Article 27

1. The Member States and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper implementation of the national provisions adopted by the Member States pursuant to this Directive, taking account of the specific features of the various sectors.

2. Member States shall make provision for trade associations and other bodies representing other categories of controllers which have drawn up draft national codes or which have the intention of amending or extending existing national codes to be able to submit them to the opinion of the national authority.

Member States shall make provision for this authority to ascertain, among other things, whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to this Directive. If it sees fit, the authority shall seek the views of data subjects or their representatives.

3. Draft Community codes, and amendments or extensions to existing Community codes, may be submitted to the Working Party referred to in Article 29. This Working Party shall determine, among other things, whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to this Directive. If it sees fit, the authority shall seek the views of data subjects or their representatives. The Commission may ensure appropriate publicity for the codes which have been approved by the Working Party.
CHAPTER VI

SUPERVISORY AUTHORITY AND WORKING PARTY ON THE

PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

Article 28 Supervisory authority

1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive.

These authorities shall act with complete independence in exercising the functions entrusted to them.

2. Each Member State shall provide that the supervisory authorities are consulted when drawing up administrative measures or regulations relating to the protection of individuals’ rights and freedoms with regard to the processing of personal data.

3. Each authority shall in particular be endowed with:

   o investigative powers, such as powers of access to data forming the subject-matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties;
   o effective powers of intervention, such as, for example, that of delivering opinions in accordance with Article 20, before processing operations are carried out and ensuring appropriate publication of such opinions, or that of ordering the blocking, erasure or destruction of data, or of imposing a temporary or definitive ban on processing, or that of warning or admonishing the controller or that of referring the matter to national parliaments or other political institutions;
   o the power to engage in legal proceedings where the national provisions adopted pursuant to this Directive have been violated or to bring these violations to the attention of the judicial authorities.

Decisions by the supervisory authority which give rise to complaints may be appealed against through the courts.

4. Each supervisory authority shall hear claims lodged by any person, or by an association representing that person, concerning the protection of his rights and freedoms in regard to the processing of personal data. The person concerned shall be informed of the outcome of the claim.

Each supervisory authority shall, in particular, hear claims for checks on the lawfulness of data processing lodged by any person when the national provisions adopted pursuant to
Article 13 of this Directive apply. The person shall at any rate be informed that a check has taken place.

5. Each supervisory authority shall draw up a report on its activities at regular intervals. The report shall be made public.

6. Each supervisory authority is competent, whatever the national law applicable to the processing in question, for exercising, on the territory of its own Member State, the powers attributed to it in accordance with paragraph 3. Each authority may be requested to exercise its powers by an authority of another Member State.

The supervisory authorities shall cooperate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information.

7. Member States shall provide that the members and staff of the supervisory authority, even after their employment has ended, are to be subject to a duty of professional secrecy with regard to confidential information to which they have access.

**Article 29 Working Party on the Protection of Individuals with regard to the Processing of Personal Data**

1. A Working Party on the Protection of Individuals with regard to the Processing of Personal Data, hereinafter referred to as "the Working Party", is hereby set up.

It shall have advisory status and act independently.

2. The Working Party shall be composed of a representative of the supervisory authority or authorities designated by each Member State and of a representative of the authority or authorities established for Community institutions and bodies, and of a representative of the Commission.

Each member of the Working Party shall be designated by the institution, authority or authorities which he represents. Where a Member State designates more than one supervisory authority, they shall nominate a joint representative. The same shall apply for the authorities established for Community institutions and bodies.

3. The Working Party shall take decisions by a simple majority of the representatives of the supervisory authorities.

4. The Working Party shall elect its chairman. The chairman's term of office shall be two years. His appointment shall be renewable.

5. The Working Party's secretariat shall be provided by the Commission.

7. The Working Party shall consider items placed on its agenda by its chairman, either on his own initiative or at the request of a representative of the supervisory authorities or at the Commission's request.

**Article 30**

1. The Working Party shall:

(a) examine any question covering the application of the national measures adopted under this Directive in order to contribute to the uniform application of such measures;

(b) give the Commission an opinion on the level of protection in the Community and in third countries;

(c) advise the Commission on any proposed amendment of this Directive, on any additional or specific measures to safeguard the rights and freedoms of natural persons with regard to the processing of personal data and on any other proposed Community measures affecting such rights and freedoms;

(d) give an opinion on codes of conduct drawn up at Community level.

2. If the Working Party finds that divergences likely to affect the equivalence of protection for persons with regard to the processing of personal data in the Community are arising between the laws or practices of Member States, it shall inform the Commission accordingly.

3. The Working Party may, on its own initiative, make recommendations on all matters relating to the protection of persons with regard to the processing of personal data in the Community.

4. The Working Party's opinions and recommendations shall be forwarded to the Commission and to the committee referred to in Article 31.

5. The Commission shall inform the Working Party of the action it has taken in response to its opinions and recommendations. It shall do so in a report which shall also be forwarded to the European Parliament and the Council. The report shall be made public.

6. The Working Party shall draw up an annual report on the situation regarding the protection of natural persons with regard to the processing of personal data in the Community and in third countries, which it shall transmit to the Commission, the European Parliament and the Council. The report shall be made public.
CHAPTER VII

COMMUNITY IMPLEMENTING MEASURES

Article 31 The Committee

1. The Commission shall be assisted by a committee composed of the representatives of the Member States and chaired by the representative of the Commission.

2. The representative of the Commission shall submit to the committee a draft of the measures to be taken. The committee shall deliver its opinion on the draft within a time limit which the chairman may lay down according to the urgency of the matter. The opinion shall be delivered by the majority laid down in Article 148(2) of the Treaty. The votes of the representatives of the Member States within the committee shall be weighted in the manner set out in that Article. The chairman shall not vote. The Commission shall adopt measures which shall apply immediately. However, if these measures are not in accordance with the opinion of the committee, they shall be communicated by the Commission to the Council forthwith. In that event:

The Commission shall defer application of the measures which it has decided for a period to be laid down in each act adopted by the Council, but which may in no case exceed three months from the date of communication.

The Council, acting by a qualified majority, may take a different decision within the time limit referred to in the previous paragraph.

FINAL PROVISIONS

Article 32

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive at the latest at the end of a period of three years from the adoption of the Directive.

When Member States adopt these measures, they shall contain a reference to this Directive or be accompanied by such reference on the occasion of their official publication. The methods of making such reference shall be laid down by the Member States.

2. Member States shall ensure that processing already underway on the date the national provisions adopted pursuant to this Directive enter into force, is brought into conformity with these provisions within 3 years of this date.

By way of derogation from the preceding subparagraph, Member States may provide that the processing of data already held in manual filing systems on the date of entry into force
of the national provisions adopted in implementation of this Directive shall be brought into conformity with Articles 6, 7 and 8 within 12 years of the date on which this Directive is adopted. Member States shall, however, grant the data subject the right to obtain, at his request and in particular at the time of exercising his right of access, the rectification, erasure or blocking of data which are incomplete, inaccurate or stored in a way incompatible with the legitimate purposes pursued by the controller.

3. By way of derogation from paragraph 2, Member States may provide, subject to suitable safeguards that data kept for the sole purpose of historical research are not brought into conformity with Articles 6, 7 and 8 of this Directive.

4. Member States shall communicate to the Commission the provisions of national law which they adopt in the field covered by this Directive.

**Article 33**

The Commission shall report to the Council and the European Parliament at regular intervals, starting not later than three years after the date referred to in Article 32(1), on the implementation of this Directive, attaching to its report, if necessary, suitable proposals for amendments. The report shall be made public.

The Commission shall examine, in particular, the application of this Directive to the data processing of sound and image data relating to natural persons and shall submit any appropriate proposals which prove to be necessary, taking account of developments in information technology and in the light of the state of progress in the information society.

**Article 34**

This Directive is addressed to the Member States

Done at Luxembourg,

For the European Parliament For the Council

The President,

K. Haensch L. Atienza Ser
Appendix 3: Privacy Act 1988 (Cth) Schedule 3, National Privacy Principles

1. Collection

1.1 An organisation must not collect personal information unless the information is necessary for one or more of its functions or activities.

1.2 An organisation must collect personal information only by lawful and fair means and not in an unreasonably intrusive way.

1.3 At or before the time (or, if that is not practicable, as soon as practicable after) an organisation collects personal information about an individual from the individual, the organisation must take reasonable steps to ensure that the individual is aware of:

   a) the identity of the organisation and how to contact it; and

   b) the fact that he or she is able to gain access to the information; and

   c) the purposes for which the information is collected;

   d) and the organisations (or the types of organisations) to which the organisation usually discloses information of that kind; and

   e) any law that requires the particular information to be collected;

   f) and the main consequences (if any) for the individual if all or part of the information is not provided.

1.4 If it is reasonable and practicable to do so, an organisation must collect personal information about an individual only from that individual.

1.5 If an organisation collects personal information about an individual from someone else, it must take reasonable steps to ensure that the individual is or has been made aware of the matters listed in subclause 1.3 except to the extent that making the individual aware of the matters would pose a serious threat to the life or health of any individual.

2. Use and disclosure

2.1 An organisation must not use or disclose personal information about an individual for a purpose (the secondary purpose) other than the primary purpose of collection unless:

1 This is an unofficial text. For the authoritative text of the National Privacy Principles, reference should be made to the Privacy Act 1988 (Cth) sch 3. Available at <http://www.law.gov.au/privacy/NPP.html>
a) both of the following apply:

i) the secondary purpose is related to the primary purpose of collection and, if the personal information is sensitive information, directly related to the primary purpose of collection;

ii) the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose; or

b) the individual has consented to the use or disclosure; or

c) if the information is not sensitive information and the use of the information is for the secondary purpose of direct marketing:

i) it is impracticable for the organisation to seek the individual's consent before that particular use; and

ii) the organisation will not charge the individual for giving effect to a request by the individual to the organisation not to receive direct marketing communications; and

iii) the individual has not made a request to the organisation not to receive direct marketing communications; and

iv) the organisation gives the individual the express opportunity at the time of first contact to express a wish not to receive any further direct marketing communications; or

d) if the information is health information and the use or disclosure is necessary for research, or the compilation or analysis of statistics, relevant to public health or public safety:

i) it is impracticable for the organisation to seek the individual's consent before the use or disclosure; and

ii) the use or disclosure is conducted in accordance with guidelines approved by the Commissioner under section 95A for the purposes of this subparagraph; and

iii) in the case of disclosure-the organisation reasonably believes that the recipient of the health information will not disclose the health information, or personal information derived from the health information; or

e) the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent:

i) a serious and imminent threat to an individual's life, health or safety; or

ii) a serious threat to public health or public safety; or
f) the organisation has reason to suspect that unlawful activity has been, is being or may be engaged in, and uses or discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities; or

g) the use or disclosure is required or authorised by or under law; or

h) the organisation reasonably believes that the use or disclosure is reasonably necessary for one or more of the following by or on behalf of an enforcement body:

i) the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law;

ii) the enforcement of laws relating to the confiscation of the proceeds of crime;

iii) the protection of the public revenue;

iv) the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct;

v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal.

Note 1: It is not intended to deter organisations from lawfully co-operating with agencies performing law enforcement functions in the performance of their functions.

Note 2: Subclause 2.1 does not override any existing legal obligations not to disclose personal information. Nothing in subclause 2.1 requires an organisation to disclose personal information; an organisation is always entitled not to disclose personal information in the absence of a legal obligation to disclose it.

Note 3: An organisation is also subject to the requirements of National Privacy Principle 9 if it transfers personal information to a person in a foreign country.

2.2 If an organisation uses or discloses personal information under paragraph 2.1 (h), it must make a written note of the use or disclosure.

2.3 Subclause 2.1 operates in relation to personal information that an organisation that is a body corporate has collected from a related body corporate as if the organisation’s primary purpose of collection of the information were the primary purpose for which the related body corporate collected the information.

2.4 Despite subclause 2.1, an organisation that provides a health service to an individual may disclose health information about the individual to a person who is responsible for the individual if:
a) the individual:
   i) is physically or legally incapable of giving consent to the disclosure; or
   ii) physically cannot communicate consent to the disclosure; and

b) a natural person (the carer) providing the health service for the organisation is satisfied that either:
   i) the disclosure is necessary to provide appropriate care or treatment of the individual; or
   ii) the disclosure is made for compassionate reasons; and

c) the disclosure is not contrary to any wish:
   i) expressed by the individual before the individual became unable to give or communicate consent; and
   ii) of which the carer is aware, or of which the carer could reasonably be expected to be aware; and

d) the disclosure is limited to the extent reasonable and necessary for a purpose mentioned in paragraph (b).

2.5 For the purposes of subclause 2.4, a person is responsible for an individual if the person is:

a) a parent of the individual; or

b) a child or sibling of the individual and at least 18 years old; or

c) a spouse or de facto spouse of the individual; or

d) a relative of the individual, at least 18 years old and a member of the individual’s household; or

e) a guardian of the individual; or

f) exercising an enduring power of attorney granted by the individual that is exercisable in relation to decisions about the individual’s health; or

g) a person who has an intimate personal relationship with the individual; or

h) a person nominated by the individual to be contacted in case of emergency.

2.6 In subclause 2.5:
child of an individual includes an adopted child, a step-child and a foster-child, of the individual.

parent of an individual includes a step-parent, adoptive parent and a foster-parent, of the individual.

relative of an individual means a grandparent, grandchild, uncle, aunt, nephew or niece, of the individual.

sibling of an individual includes a half-brother, half-sister, adoptive brother, adoptive sister, step-brother, step-sister, foster-brother and foster-sister, of the individual.

3 Data quality

An organisation must take reasonable steps to make sure that the personal information it collects, uses, or discloses is accurate, complete and up-to-date.

4 Data security

4.1 An organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.

4.2 An organisation must take reasonable steps to destroy or permanently deidentify personal information if it is no longer needed for any purpose for which the information may be used or disclosed under National Privacy Principle 2.

5 Openness

5.1 An organisation must set out in a document clearly expressed policies on its management of personal information. The organisation must make the document available to anyone who asks for it.

5.2 On request by a person, an organisation must take reasonable steps to let the person know, generally, what sort of personal information it holds, for what purposes, and how it collects, holds, uses and discloses that information.

6 Access and correction

6.1 If an organisation holds personal information about an individual, it must provide the individual with access to the information on request by the individual, except to the extent that:

a) in the case of personal information other than health information providing access would pose a serious and imminent threat to the life or health of any individual; or
b) in the case of health information-providing access would pose a serious threat to the life or health of any individual; or

c) providing access would have an unreasonable impact upon the privacy of other individuals; or

d) the request for access is frivolous or vexatious; or

e) the information relates to existing or anticipated legal proceedings between the organisation and the individual, and the information would not be accessible by the process of discovery in those proceedings; or

f) providing access would reveal the intentions of the organisation in relation to negotiations with the individual in such a way as to prejudice those negotiations; or

g) providing access would be unlawful; or

h) denying access is required or authorised by or under law; or

i) providing access would be likely to prejudice an investigation of possible unlawful activity; or

j) providing access would be likely to prejudice:

i) the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law; or

ii) the enforcement of laws relating to the confiscation of the proceeds of crime; or

iii) the protection of the public revenue; or

iv) the prevention, detection, investigation orremedying of seriously improper conduct or prescribed conduct; or

v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of its orders; by or on behalf of an enforcement body; or

k) an enforcement body performing a lawful security function asks the organisation not to provide access to the information on the basis that providing access would be likely to cause damage to the security of Australia.

6.2 However, where providing access would reveal evaluative information generated within the organisation in connection with a commercially sensitive decision-making process, the organisation may give the individual an explanation for the commercially sensitive decision rather than direct access to the information.
Note: An organisation breaches subclause 6.1 if it relies on subclause 6.2 to give an individual an explanation for a commercially sensitive decision in circumstances where subclause 6.2 does not apply.

6.3 If the organisation is not required to provide the individual with access to the information because of one or more of paragraphs 6.1(a) to (k) (inclusive), the organisation must, if reasonable, consider whether the use of mutually agreed intermediaries would allow sufficient access to meet the needs of both parties.

6.4 If an organisation charges for providing access to personal information, those charges:

a) must not be excessive; and

b) must not apply to lodging a request for access.

6.5 If an organisation holds personal information about an individual and the individual is able to establish that the information is not accurate, complete and up to date, the organisation must take reasonable steps to correct the information so that it is accurate, complete and up-to-date.

6.6 If the individual and the organisation disagree about whether the information is accurate, complete and up-to-date, and the individual asks the organisation to associate with the information a statement claiming that the information is not accurate, complete or up-to-date, the organisation must take reasonable steps to do so.

6.7 An organisation must provide reasons for denial of access or a refusal to correct personal information.

7 Identifiers

7.1 An organisation must not adopt as its own identifier of an individual an identifier of the individual that has been assigned by:

a) an agency; or

b) an agent of an agency acting in its capacity as agent; or

c) a contracted service provider for a Commonwealth contract acting in its capacity as contracted service provider for that contract.

7.2 An organisation must not use or disclose an identifier assigned to an individual by an agency, or by an agent or contracted service provider mentioned in subclause 7.1, unless:

a) the use or disclosure is necessary for the organisation to fulfil its obligations to the agency; or
b) one or more of paragraphs 2.1(e) to 2.1(h) (inclusive) applies to the use or disclosure.

7.3 In this clause:

**identifier** includes a number assigned by an organisation to an individual to identify uniquely the individual for the purposes of the organisation’s operations. However, an individual’s name is not an **identifier**.

8 Anonymity

Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation.

9 Transborder data flows

An organisation in Australia or an external Territory may transfer personal information about an individual to someone (other than the organisation or the individual) who is in a foreign country only if:

a) the organisation reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the information that are substantially similar to the National Privacy Principles; or

b) the individual consents to the transfer; or

c) the transfer is necessary for the performance of a contract between the individual and the organisation, or for the implementation of pre-contractual measures taken in response to the individual’s request; or

d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the organisation and a third party; or

e) all of the following apply:

i) the transfer is for the benefit of the individual;

ii) it is impracticable to obtain the consent of the individual to that transfer;

iii) if it were practicable to obtain such consent, the individual would be likely to give it; or

f) the organisation has taken reasonable steps to ensure that the information which it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with the National Privacy Principles.
10 Sensitive information

10.1 An organisation must not collect sensitive information about an individual unless:

a) the individual has consented; or

b) the collection is required by law; or

c) the collection is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual, where the individual whom the information concerns:

i) is physically or legally incapable of giving consent to the collection; or

ii) physically cannot communicate consent to the collection; or

d) if the information is collected in the course of the activities of a non-profit organisation-the following conditions are satisfied:

i) the information relates solely to the members of the organisation or to individuals who have regular contact with it in connection with its activities;

ii) at or before the time of collecting the information, the organisation undertakes to the individual whom the information concerns that the organisation will not disclose the information without the individual’s consent; or

e) the collection is necessary for the establishment, exercise or defence of a legal or equitable claim.

10.2 Despite subclause 10.1, an organisation may collect health information about an individual if:

a) the information is necessary to provide a health service to the individual; and

b) the information is collected:

i) as required by law (other than this Act); or

ii) in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation.

10.3 Despite subclause 10.1, an organisation may collect health information about an individual if:

a) the collection is necessary for any of the following purposes:

i) research relevant to public health or public safety;
ii) the compilation or analysis of statistics relevant to public health or public safety;

iii) the management, funding or monitoring of a health service; and

b) that purpose cannot be served by the collection of information that does not identify the individual or from which the individual’s identity cannot reasonably be ascertained; and

c) it is impracticable for the organisation to seek the individual's consent to the collection; and

d) the information is collected:

i) as required by law (other than this Act); or

ii) in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation; or

iii) in accordance with guidelines approved by the Commissioner under section 95A for the purposes of this subparagraph.

10.4 If an organisation collects health information about an individual in accordance with subclause 10.3, the organisation must take reasonable steps to permanently deidentify the information before the organisation discloses it.

10.5 In this clause:

**non-profit organisation** means a non-profit organisation that has only racial, ethnic, political, religious, philosophical, professional, trade, or trade union aims.