Background and Overview of Law in Australia

Job: research/pic/allvols/serv_0/back_263013
Page: **1** Date: **18/8/2011** Time: **10:50:27**
bwpageid:: 1::
bwservice::0::

Job: research/pic/allvols/serv_0/back_263013
Page: **2** Date: **18/8/2011** Time: **10:50:27**
bwpageid:: 2::
bwservice::0::

Background and Overview

[1000] Introduction

In 2007 Deakin University law academic Mirko Bagaric stated that—

> privacy is a middle-class invention by people with nothing else to worry about. Normally they would have every right to live in their moral fog, but not when their confusion permeates the feeble minds of law-makers and puts the innocent at risk.
>
> The right to privacy is the adult equivalent of Santa Claus and unicorns. No one has yet been able to identify where the right to privacy comes from and why we need it. In fact, the right to privacy is destructive of our wellbeing. It prevents us attaining things that really matter, such as safety and security and makes us fear one another.
>
> A strong right to privacy is no more than a request for secrecy — refuge of the guilty, paranoid and misguided, none of whom should be heeded in sorting through the moral priorities of the community.[1]

Australian courts, legislators and citizens — middle-class or otherwise — disagree with Dr Bagaric. That is evident in over a hundred statutes that are specifically concerned with privacy and data protection or that feature privacy provisions. It is also evident in common law about confidentiality. Finally, it is evident in claims by advocacy groups and in the concerns of ordinary people who use health services, buy products online, encounter paparazzi, complete a census form, use a passport, experience workplace surveillance or receive income support.

This service is a guide for realists. It is written for legal practitioners, public/private sector managers, policy-makers and academics who deal with the realities of law about privacy, data protection and confidentiality. That law is complex. It is dynamic. It is not a phantom such as the unicorn or the tooth fairy. It is not going to disappear. It affects the operation of business, not-for-profit bodies and government agencies. It involves litigation by individuals and businesses. It also involves penalties, whether in terms of fines imposed by regulators and courts or in terms of reputational damage.

Notes

1 Mirko Bagaric (2007), 'Privacy Is The Last Thing We Need', *The Age* 22 April 2007. Dr Bagaric is co-author of *Privacy Law in Australia* (Leichhardt: Federation Press 2005). His disquiet regarding privacy is evident in ABC Radio National, 'The Law Report: Criminals and Privacy' (28 March 2006) at www.abc.net.au/rn/lawreport/stories/2006/1601294.htm.

[1010] Orientation

This service has a practice and procedure focus, with an emphasis on "what is the law", "what do I need to do" and "how do I do it".

It does not provide an exhaustive academic treatment of the subject. Instead it aims to provide a concise, practical and easy-to-navigate source of guidance on application of the law.

The intention is that each guide card contains the information necessary for a lawyer to understand what considerations should be taken into account and how they could be addressed, highlighting traps or tips.

The intention is also to provide enough legal context so that practitioners can identify

Job: research/pic/allvols/serv_0/back_263013
Page: **3** Date: **18/8/2011** Time: **10:50:27**
bwpageid:: 3::
bwservice::0::

potential problems before they occur. Some chapters accordingly look ahead to how the law is likely to develop in the next couple of years, rather than solely looking backwards to past cases and statutes.

[1020] Structure of the Service

The service has 11 chapters, as follows.

Guide card	**Topics covered**
Background and overview of law in Australia	• Overview of privacy landscape • Key statutes • Key players
Key Principles and concepts in Privacy, Confidentiality and Data Security	• Key concepts and principles • Operational challenges • Harms • Remedies
Investigations and Complaints	• Investigation of complaints under privacy statutes • Overview of Commonwealth Privacy Commissioner and state commissioners • Acting for a complainant/respondent • Negotiating a settlement • Enforcement
Regulation of credit reporting information and activities	• Credit reporting
Approved privacy codes	• Privacy and confidentiality in emergencies and disasters • Private sector management of information • Obligations of confidence • Data matching
Private sector — data management, confidentiality and compliance policies	• Practical issues • Privacy audits • Privacy policies • Privacy collection notices • Consent • Complaint handling procedures • Data Breaches • Portable storage devices • Discovery
Industry specific FAQs	• Health services • Superannuation • Financial services • Insurance • Direct marketing • Education • Miscellaneous

Job: research/pic/allvols/serv_0/back_263013
Page: **4** Date: **18/8/2011** Time: **10:50:28**
bwpageid:: 4::
bwservice::0::

	• Public sector • Collections to and disclosures from other agencies • Public registers • Disclosures to State agencies • Disclosures regarding APS Code of Conduct matters • Disclosures for medical research • Handling unsolicited information
Health Records	• Obtaining health information • Right to access • Complaints • Retention of information • Securing information • Electronic health records • Genetic information • Future concerns
Laws of Confidence	• Breach of confidence • Spent convictions • Human rights legislation • Direct marketing laws • Employment law and employee privacy • Listening and surveillance devices • Monitoring workplace computers, emails and internet Monitoring staff use of telephones • Workplace video surveillance • Biometric access controls and logs • Drug and alcohol testing • DNA testing
Annotated Privacy Act and other key legislation	• Annotated Privacy Act (Cth) • Guide to other key legislation
Annotated National Privacy Principles	• Annotated National Privacy Principles

Chapter 1 Background and overview of law in Australia

The chapter provides an introduction to the overall service and an overview of the privacy landscape, highlighting key statutes and actors. (There is a more detailed outline of the chapter below.)

Chapter 2 Key Principles and Concepts in Privacy, Confidentiality and Data Security

The chapter introduces key concepts and principles, which are unpacked in the following chapters in guidance about specific statutory provisions, cases and operational challenges. It includes a discussion of harms and remedies.

Chapter 3 Investigations and Complaints

The chapter deals with investigation of complaints under the key privacy statutes. It

Job: research/pic/allvols/serv_0/back_263013
Page: **5** Date: **18/8/2011** Time: **10:50:28**
bwpageid:: 5::
bwservice::0::

provides an overview of the investigation process that is used by the Commonwealth Privacy Commissioner and state Commissioners. It highlights the Commissioner's powers and approach. It then offers guidance on acting for a complainant and acting for a respondent in relation to breaches of the privacy statutes. The chapter includes guidance on negotiating a settlement and on enforcement.

Chapter 4 Regulation of specific information and activities

The chapter provides in-depth guidance about privacy law regarding specific information/activities, centred on Commonwealth law. That guidance relates to credit reporting, the handling of Tax File Number information and Data-matching.

Chapter 5 Approved Privacy Codes

The chapter deals with the approved privacy codes. It considers privacy and confidentiality aspects of emergencies and disasters, the management of information in the public sector and by contractors within an emergency framework, obligations of confidence and data matching.

Chapter 6 Private sector — data management, confidentiality and compliance policies

As the title indicates, the chapter provides an introduction to privacy and confidentiality in the private sector, including financial and medical information. It offers guidance on principles and practicalities that are significant for non-government bodies, for example the meaning of consent in relation to privacy and the handling of data breaches. The chapter discusses small business opting-in to requirements that are mandated for large organisations and the framework for government contractors.

Its guidance on practical issues covers privacy audits, formal privacy policies and privacy collection notices, privacy consent forms, privacy impact assessments and complaint handling procedures. It also covers questions about electronic commerce, customer profiling, the management of portable devices and data breaches, human resource management (in particular privacy aspects of recruitment), contractor and agent relationships, collection of data from young people, the discovery of documents in legal proceedings and the framework for the protection of personal information where a business is sold.

Chapter 7 Industry specific FAQs

The chapter provides sector-specific guidance for legal practitioners and managers regarding health services, superannuation, financial services, insurance, direct marketing and education.

It also covers what readers need to know about questions regarding public sector information handling, including collection by and disclosures from other agencies, the management of public registers, disclosures to State/Territory agencies, disclosures regarding APS Code of Conduct matters, the handling of unsolicited information and disclosures for medical research.

Chapter 8 Health records legislation

The chapter considers health records, subject to the national privacy statute and different legislative requirements in each jurisdiction. It offers guidance on obtaining health information (including the legislative requirements regarding rights of access), the complaints frameworks (identifying legislative requirements in each jurisdiction), the statutory requirements for retention of information and for securing information. The

Job: research/pic/allvols/serv_0/back_263013
Page: **6** Date: **18/8/2011** Time: **10:50:28**
bwpageid:: 6::
bwservice::0::

chapter includes examination of questions regarding electronic health records and capacity. It also discusses emerging issues regarding genetic information and privacy aspects of new technologies.

Chapter 9 Laws of confidence

Privacy statutes co-exist with a substantial body of law regarding breach of confidence, employment, law enforcement and justice. That law is increasingly being tied to national and State/Territory human rights frameworks. The chapter offers guidance on breach of confidence, spent convictions and direct marketing codes.

It identifies the law and addresses specific practice questions regarding workplace privacy, including the use of listening and other surveillance devices, the monitoring of workplace computers and communications (eg employer examination of email, phone calls and web surfing), protocols for biometric access controls, employee drug and alcohol testing, and emerging issues regarding DNA testing.

Chapters 10 and 11 Key Legislation and National Privacy Principles

As a guide for readers the discussion in the preceding chapters is supported through the identification of the key Commonwealth, State and Territory privacy and data protection statutes, offering an at-a-glance picture of the major legislation. That inventory is accompanied by identification of the national industry codes regarding privacy and by the text of the National Privacy Principles.

[1030] Overview

This section provides a context for discussion in the following chapters regarding specific statutes, codes, cases and operational issues.

It is aimed at readers who have an interest in the law of privacy and confidentiality but do not have in-depth expertise. Readers with a comprehensive understanding of the law may wish to move directly to specific chapters later in this book.

It is also aimed at readers who are familiar with a specific Commonwealth or state/territory statute but have the need to extend their understanding to law in a different jurisdiction or industry, or who want some sense of how the law is likely to develop in future (so that they can, for example, anticipate change in advising clients/employers about forward-looking protocols for data handling).

The following paragraphs begin by identifying the three key concepts (privacy, confidentiality and data protection) dealt with in this work. Those concepts are explored in the following chapter, which discusses information principles — articulated in Commonwealth and State/Territory privacy statutes and reflected in industry codes — and how Australian courts have addressed the concepts in common law and in interpreting the various statutes.

This chapter then moves on to offer a picture of the regulatory framework regarding privacy and data protection, noting the absence of an explicit constitutional basis and the significance of industry codes implemented under co-regulatory schemes. It next offers an overview of different public and private sector bodies that develop and implement privacy law or that shape future law through analysis and advocacy.

The chapter then characterises how privacy law operates in Australia, highlighting the sectoral (industry-specific) and jurisdiction-specific patchwork of statutes that interacts with dat by day practice and common law. Privacy law in Australia is dynamic and substantial change can be expected in future, reflecting developments in technologies (eg biometric identity verification, geolocation services and social network services such as Facebook), tighter regulation in key trading partners such as the European Union and emerging consumer perceptions of rights, risks, remedies and responsibilities.

Job: research/pic/allvols/serv_0/back_263013
Page: 7 Date: 18/8/2011 Time: 10:50:28
bwpageid:: 7::
bwservice::0::

An outline of the Commonwealth regime is then provided, with a synopsis of the Privacy Act 1988 (Cth) and key privacy or data protection provisions in other statutes. It is important to recognise that Commonwealth privacy law involves a range of enactments. Those statutes and associated codes are examined in detail in the second half of this service.

Other jurisdictions in Australia have implemented and are continuing to develop privacy or information law that exists alongside the Commonwealth regime and that in practice is often stronger than the Privacy Act 1988 (Cth). An understanding of relevant State/Territory law may be particularly significant in advising organisations or in representing clients seeking remedies for action under non-Commonwealth privacy statutes.

The chapter next identifies international data protection frameworks (for example the OECD data protection Guidelines and salient European Union data protection Directives) and points to overseas models, notably law in the UK, US and Canada. Those frameworks are important for Australian entities that trade across borders or are engaged in the offshoring of data handling (for example major retailers, financial institutions and even academic institutions).

This chapter concludes with a discussion of what forces are driving privacy law development and how both law and practice are likely to change in future. An awareness of drivers and likely directions means that organisations in the public and private sectors are in a position to minimise reputational damage and to embody best practice when establishing information management systems, for example avoiding the problems faced by Sony through unauthorised access in 2011 to records of over 70 million customers.

[1100] Making sense of Privacy, Confidentiality and Data Protection

What is privacy? As the quotation at the beginning of this chapter indicated, it is something about which people disagree.

They often disagree strongly about principles or about priorities, for example that privacy at an abstract level is an individual and social good but something that should be sacrificed in order to facilitate other goods such as effective national security, minimisation of insurance fraud, reduction of risk of offences by sexual offenders, or encouragement of genetic research regarding cancer, dementia or other conditions. Proponents of privacy have characterised it as a fundamental human right (a characterisation that has some recognition in Australian law) and as something that is sufficiently valued by the Australian community to be given a statutory basis in the different jurisdictions, albeit on an uneven and changing basis.

Disagreement about privacy is not surprising, given the patchy nature of statutory and common law protection — law and the media shape perceptions. It is also unsurprising given uncertainty about the language of privacy and thence rules, harms and remedies. Australian law continues to grapple with questions about whether privacy is independent of context (essentially a broad right to be left to live without inappropriate interference). Should privacy instead be conceptualised in terms of—

- bodily privacy (for example a freedom from being manually searched or imaged using x-ray and other technologies at airports),
- territorial or locational privacy principles (a freedom from being individually observed or mapped, such as trespass onto your land or premises, photography by your nosy neighbour over the back fence, inclusion of images in services such as Google StreetView or tracking as you travel on roads, trains and planes),
- information privacy principles (a broader right to control information created by or about yourself, such as restrictions on what personal data is held in a paper or

Job: research/pic/allvols/serv_0/back_263013
Page: 8 Date: 18/8/2011 Time: 10:50:28
bwpageid:: 8::
bwservice::0::

computer file and who gets to access that file or what information about you can appear in newspapers and on television),
- types of information (for example "intimate" versus "public", sensitive versus non-sensitive, financial, medical, restricted to an individual versus identifying an affinity group such as ethno-religious affiliation),
- surveillance technologies (telecommunications, cameras, listening devices) or situations (eg the home, streets and other public places, the workplace).

Those questions overlap with much past law, which for example includes offences regarding assault, stalking, nuisance, computer hacking or misuse of the telegraphic network and injunctions addressing infringement of copyright through unauthorised publication of personal letters or diaries.

They also overlap with disagreements about harms and remedies regarding confidentiality, for example personal information imparted to a medical or legal practitioner in the expectation that it will not be divulged to a third party, and with uncertainty about the effective protection of data in a world of hackers, lost USB drives and leaky firewalls.

Privacy, confidentiality and data protection as concepts are discussed in the following chapter. That chapter examines the specific privacy principles that are articulated in international agreements (such as the 1981 OECD data protection Guidelines and the Universal Declaration of Human Rights) and that are express features of major Australian privacy statutes.

Community attitudes are inconsistent. Specialists have, for example, noted that although many people claim to be deeply committed to privacy those same people are consumers of mass media founded on intrusion into the private lives of celebrities and will supply intimate information about their own lives to marketers or to fellow participants in social network services.

One response is that it is clear that attitudes are changing (with some demographics increasingly voicing strong concerns about particular technologies or practices) and that people will often express a quite visceral hostility to disregard of their own privacy. Some of that hostility is deeply traditional and is evident for example in statutes regarding "peeping toms" or other unauthorised surveillance that predates electronic databases or contemporary developments such as "sexting" by teenagers with webcams and mobile phones. Strong feelings about privacy are also evident in criticisms of proposals for an Australia Card and of biometric registration schemes, albeit the vehemence with which some claims were expressed was inverse proportional to the advocate's understanding of law and technology. It has *not* however been reflected in recognition of a broad common law tort of privacy, although the High Court in *Lenah Game Meats*[2] did not rule out the future development of such a tort and various law reform bodies have recommended establishment of a statutory cause of action.[3]

Irrespective of confusion among the community and disagreement among managers and legal practitioners it is a fact that Australian law broadly seeks to protect privacy and confidentiality.

That law encompasses data protection, going beyond the collection of information — surreptitiously or otherwise — and establishing requirements regarding the safeguarding of that personal information, for example restrictions on its unauthorised provision to third parties and expectations about its proper disposal. Law regarding data protection is broad, for example criminalising unauthorised access to, use of, dissemination of or destruction/modification of information on electronic databases. Not all of the data that is covered by data protection law is personal and thus of concern in relation to privacy. Cybercrime statutes could for example address access by a hacker to a corporate server

Job: research/pic/allvols/serv_0/back_263013
Page: **9** Date: **18/8/2011** Time: **10:50:28**
bwpageid:: 9::
bwservice::0::

that contains architectural blueprints or chemical test data. International agreements have increasing extended beyond protection of personal data to encompass protection of confidential information in digital formats.[4]

Notes

2 *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199; 185 ALR 1; [2001] HCA 63; BC200107043. See also *Hosking v Runting* (2004) 7 HRNZ 301; [2005] 1 NZLR 1 at 59.

3 Australian Law Reform Commission (2008), *For Your Information: Australian Privacy Law & Practice* (ALRC Report 108) recommendation 74, Victorian Law Reform Commission (2010), *Surveillance in Public Places — Final Report* (report 18) 150 and New South Wales Law Reform Commission (2009), *Invasion of Privacy* (report 120) 4.11.

4 See for example the Council of Europe Cybercrime Convention, reflected in the *Cybercrime Legislation Amendment Bill 2011* (Cth). An introduction to the Convention is provided in Brenner S (2007) 'The Council of Europe's Convention on Cybercrime' in Balkin J [ed] *Cybercrime* (New York: New York University Press).

[1150] Background to the regulatory framework

The framework for privacy in Australia is complex and, as discussed below, is changing.

The framework has three aspects: law, industry codes and practice on the part of individuals and organisations in the public and private sectors. It embodies efforts to achieve a balance between the rights of individuals and those of public, recognising the innate dignity of each person and benefits for society, organisations and individuals in sharing information.

[1175] Law

There is no express reference to privacy or data protection in the Commonwealth Constitution and no unambiguous head of power for privacy legislation.[5] That absence reflects both the priorities of the Federation Fathers (in essence the articulation of intergovernmental relations) and an assumption that common law would address all significant needs in a way that did not crimp individual liberty or the operation of organisations. It might also have reflected a lack of imagination on the part of the Fathers, although the history of Australian telecommunications and postal statutes prior to 1900 indicates that the importance of confidentiality was recognised.

Privacy protection in Australia is thus a creature of statute law and common law rather than something founded on a specific reference in the Commonwealth Constitution and enshrined by the High Court in decisions regarding that Constitution. Privacy is recognised in the Charter of Human Rights and Responsibilities Act 2006 (Vic) s 13 and the Human Rights Act 2004 (ACT) s 12 but is not an express feature of the state/territory constitutions.

Instead, as highlighted below, the Australian jurisdictions have enacted laws that are concerned with privacy at a broad level, for example the Privacy Act 1988 (Cth) and Information Privacy Act 2009 (Qld), or that deal with particular sectors or activities, for example the Listening Devices Act 1991 (Tas), Workplace Privacy Act 2010 (ACT) and the Health Records (Privacy and Access) Act 1997 (ACT).[6]

A wide range of Commonwealth, State and Territory enactments feature provisions that protect confidentiality by restricting unauthorised disclosure of personal information or that embody a respect for the individual through non-recognition of some information. Examples of such statutes are the Telecommunications Act 1997 (Cth) s 270, the Census and Statistics Act 1905 (Cth) ss 13 and 19A, the Archives Act 1983 (Cth) s 33, the Spent Convictions Act 1988 (WA), the Adoption Act 1988 (SA) ss 24 and 27.

Job: research/pic/allvols/serv_0/back_263013
Page: **10** Date: **18/8/2011** Time: **10:50:28**
bwpageid:: 10::
bwservice::0::

A feature of much Australian legislation is provision for disclosure to law enforcement or other entities of personal information that would otherwise be restricted. That "back door" typically is concerned with national security, policing of criminal offences and action where an individual's wellbeing is threatened (for example disclosure of network information in instances of natural disaster). Examples are the Information Privacy Act 2000 (Vic) s 13, Surveillance Devices Act 2004 (Cth), the Telecommunications (Interception and Access) Act 1979 (Cth), Surveillance Devices Act 2008 (NSW), Privacy Act 1988 (Cth) s 80P and the Customs Amendment (Serious Drugs Detection) Act 2011 (Cth).

The statutes have not comprehensively replaced common law. That law remains relevant, particularly as it does not provide an exhaustive right of privacy or what has been variously characterised as publicity or personality rights.[7]

It does not, for example, prevent street photography and cases such as *Grosse v Purvis* (2003)[8] and *Doe v ABC* (2007)[9] have attracted more attention from law students than support from Australian courts. It is important to note that the High Court's judgment in *Victoria Park v Taylor* (1937)[10] was concerned with the use of information rather than with an invasion of privacy as such, although it is often incorrectly perceived as the Court definitively ruling out a tort of privacy. Common law protection for privacy centres on breach of confidence, ie misuse or threatened misuse of information that is not publicly known, is imparted on the basis of confidence (for example to a medical practitioner or partner)[11] and for which there is a reasonable expectation that the confidence will be respected.

Notes

5 The constitutional basis of the Privacy Act 1988 (Cth) has not been judicially challenged. The relevant head of power is s 51(1)(xxix) "external affairs", with the Commonwealth potentially referring to the *International Covenant on Civil and Political Rights* and the *Universal Declaration of Human Rights* among other international agreements. Salient agreements are highlighted below.

6 Consistent with s 109 of the Constitution, state law regarding privacy, data protection and confidentiality exists alongside Commonwealth statutes except where it conflicts with the Commonwealth legislative power.

7 Loughlin P, McDonald P and Van Krieken R (2010), *Celebrity and the Law* (Leichhardt: Federation Press)

8 *Grosse v Purvis* (2003) Aust Torts Reports 81-706; [2003] QDC 151.

9 *Doe v Australian Broadcasting Corp* [2007] VCC 281. See also *Kalaba v Commonwealth* [2004] FCAFC 326; BC200408581 and *Gee v Burger* [2009] NSWSC 149; BC200901601.

10 *Victoria Park Racing and Recreation Grounds Co Ltd v Taylor* (1937) 58 CLR 479; [1937] ALR 597; (1937) 1A IPR 308; BC3700015.

11 See for example *Argyll v Argyll* [1962] SC (HL) 88 and *Giller v Procopets* [2004] VSC 113; BC200402552.

[1200] Industry Codes

Much Australian privacy law involves co-regulatory schemes, ie where the private sector (typically acting through a peak industry body) develops formal codes of practice that are recognised in pertinent statutes and have a legal effect under those statutes. Co-regulation of privacy provides industry with substantial autonomy. It has been claimed to offer a flexibility and an effectiveness that is unavailable in schemes that are wholly devised and administered by privacy officials or by officials who supervise particular industries, for example telecommunications, banking and health.

It has been criticised as necessarily biased towards the interests of industry and the academia, especially major players, at the expense of consumers. It has also been

Job: research/pic/allvols/serv_0/back_263013
Page: **11** Date: **18/8/2011** Time: **10:50:28**
bwpageid:: 11::
bwservice::0::

criticised as reinforcing incapacity on the part of privacy agencies, which lack expertise and on occasion the will to deal with how the privacy principles embodied in statutes are actually implemented on a day by day basis. Future development of privacy law in Australia is likely to feature debate about the efficacy of industry codes and the co-regulatory process.

As discussed in more detail below and in Ch 3.4, much privacy law in Australia is highly sectoral, with for example discrete regimes for health privacy, telecommunications privacy and banking privacy. Those "silos" feature discrete industry codes. Although the codes are broadly consistent their expression varies, potentially resulting in confusion on the part of consumers and inconsistency in administration by organisations. There is no "one-stop-shop" regarding codes and in advising or representing clients it is important for legal practitioners to identify the relevant code and identify any relevant industry ombudsman.

[1225] Practice

The beginning of this section commented that privacy practice is important. What actually takes place, irrespective of formal legal requirements, is important for three reasons.

The first is that although some consumers have a strong "privacy consciousness" few have much sense of the law and indeed, along with some practitioners, may have difficulty discerning the relevant Commonwealth, state or territory statute or common law precedent. Perceptions of privacy law among some advocates and journalists are strongly influenced by US legal frameworks that are not applicable in Australia.

On occasion it will be appropriate to warn adults and minors that Australian law does not provide an effective remedy for misuse of personal information in a global digital environment. People should for example act defensively when sharing information on social network services such as Facebook that are based overseas, feature volatile terms and conditions and are readily accessible by individuals who may disregard legal sanctions for misbehaviour.

The second reason is that privacy law in Australia is dynamic rather than static. There are differences across jurisdictions, a challenge for businesses that operate in several locations. The Commonwealth, states and territories play "catch-up" with each other and with overseas peers. A proactive approach to privacy management will be advantageous for organisations as the privacy environment changes, ie law reform takes place and consumer sensitivity increases.

The third is that legal practitioners (and managers or consultants reading this service) may be called upon to develop and implement operational guidelines for staff and contractors who seek, handle and dispose of information about consumers. Coherent, readily accessible and easy to understand guidelines can save organisations from litigation and from reputational damage. Irrespective of legal niceties (and the small financial penalties imposed for some privacy breaches), it is best to avoid regulators, the media and the courts if you can.

Implementation of those guidelines should be intelligent. One reason for community confusion is that "front of office" staff and middle management in many public and private sector organisations use privacy as an excuse. It is common to encounter claims that "we can't help you because of privacy" or "the privacy act doesn't allow us to do that" in contexts where the legislation is not restrictive and where misuse by data custodians frustrates consumers who have a legitimate right to information about themselves or who have a right of access to government information through Freedom of Information statutes.

Job: research/pic/allvols/serv_0/back_263013
Page: **12** Date: **18/8/2011** Time: **10:50:28**
bwpageid:: 12::
bwservice::0::

[1500] Who is who

One way to make sense of current and future law about privacy, confidentiality and data protection in Australia is to look at the actors.

What government agencies and advocacy bodies are shaping the law and potentially affecting what you do as a legal practitioner, manager or policy-maker? What are their responsibilities? What are their objectives and limitations? Do they need to be taken seriously?

[1525] Understanding the actors

Contrary to some community perceptions (and suggestions by particular advocacy groups) there is no single privacy regulator with comprehensive powers and responsibilities. Beware of simplistic identifications of industry, official and consumer interests.

The privacy environment involves the interaction of courts, tribunals (some of which are especially important, for example in dealing with claims under state health privacy schemes), law reform bodies, specialist privacy watchdogs (many of which are being absorbed by information commissioners that have responsibility for freedom of information and other schemes), civil society advocacy groups, consumers, competing commercial interests (often represented by industry bodies and displaying distinct tensions between different industry sectors) and associated industry regulators (which may have experienced substantial bureaucratic capture and thus have different priorities to those of the privacy agencies).

An example of that interaction was the 2011 national round table on consumer credit reporting codes, under the auspices of the Department of Prime Minister & Cabinet and the Commonwealth Privacy Commissioner, where owners of different industry codes were at odds and the meeting ultimately resulted in an agreement to disagree while different bureaucratic, civil society and business interests pursued their own agendas.

[1550] Privacy watchdogs

From a practitioner perspective the official privacy watchdogs are important. That is for two reasons. The first is that they develop privacy codes covering the public sector and work with private sector entities in the development of private sector codes as part of the co-regulatory regimes. The second is that the watchdogs receive complaints about privacy breaches, may investigate complaints and on occasion impose penalties or criticise the behaviour of public/private sector bodies.

The shape of the watchdogs and their operating style varies considerably. State agencies in NSW and Victoria for example have been described as more activist than the Commonwealth Privacy Commissioner, which has faced criticism for being slow to respond to problems under the Privacy Act 1988 (Cth).

Initially, the Commonwealth, the States and mainland Territories tended to establish discrete Privacy Commissioners — specialist government agencies with a small staff (often predominantly without legal qualifications) headed by a distinguished former legal practitioner. Those agencies had a narrow focus and were often poorly funded. Over the past two years several have been absorbed by Information Commissioners with broader functions, for example the Office of the Information Commissioner in Queensland[12] and the Northern Territory.[13] In particular the Commonwealth Privacy Commissioner is now an arm of the Office of the Australian Information Commissioner (OAIC), a body that includes responsibility for Commonwealth Freedom of Information law. That development emulates practice overseas, notably the establishment of the Information Commissioner in the United Kingdom.

Job: research/pic/allvols/serv_0/back_263013
Page: **13** Date: **18/8/2011** Time: **10:50:28**
bwpageid:: 13::
bwservice::0::

Legal practitioners should accordingly note that the name and contact details of some watchdogs may have changed. That is particularly important because the websites of some bodies are still playing "catch-up". Contact details are provided below.

The public and private sector ombudsman offices may be significant in dealing with privacy problems. That is because the ombudsman schemes are a non-adversarial way of dealing with complaints (in the public sector typically by referring problems to the relevant Privacy Commissioner). More importantly, Ombudsmen have published reports that criticise the performance of agencies and even call for prosecutions under criminal law. An example is the 2011 Ombudsman Victoria report on an *Investigation into the Improper Release of Autopsy Information by the Victorian Institute of Forensic Medicine*.[14] If you are advising a public or private sector client the significance of the Ombudsman regarding privacy will depend on your jurisdiction: some agencies are more active than others.

Tribunals are significant in some jurisdictions, with the Administrative Decisions Tribunal in NSW for example recurrently criticising practice in the public health sector and ordering corrective action along with apologies to individuals whose privacy has been breached.[15] The costs involved in hearing by tribunals may be small relative to awards by courts in cases of assault or breach of confidence but reputational damage may be significant.[16] More detailed guidance is offered in Chs 3.4 and 3.7.

Parliamentary committees act as watchdogs in Australia. From a practitioner perspective they are potentially significant because although they cannot impose formal sanctions on public and private sector bodies their investigations may gain media attention and they can inflict reputational damage regarding the activity of businesses and government agencies. They will not take legal action against your client but their scrutiny may injure the client's public profile.[17] Finally, some non-specialist agencies, such as the Australian National Audit Office, may shed light on privacy and data protection practice within government agencies.[18]

Notes

12 www.oic.qld.gov.au.

13 www.infocomm.nt.gov.au.

14 www.ombudsman.vic.gov.au/resources/documents/Investigation_into_the_improper_release_of_autopsy_information_by_a_VIFM_employee.pdf.

15 *QB v Greater Southern Area Health Service* [2011] NSWADT 90.

16 The plaintiff in *Giller v Procopets* [2004] VSC 113; BC200402552 was for example awarded $40,000 damages were for breach of confidence, including $10,000 as compensation for humiliation and distress. The damages were not attributable to infringement of a broad right of privacy.

17 Recent Australian parliamentary committee reports of interest include the Senate Environment and Communications References Committee (2011) *The Adequacy of Protections for the Privacy of Australians Online*, Joint Select Committee on Cyber-Safety (2011), *High-Wire Act: Cyber-Safety and the Young* (Interim Report), Senate Finance and Public Administration Committee (2011), *Exposure Drafts of the Australian Privacy Amendment Legislation* (Report 1: Australian Privacy Principles) and Joint Committee on Law Enforcement (2011), *Inquiry into the adequacy of Aviation and Maritime Security Measures to combat serious and organised crime*.

18 See for example Australian National Audit Office (2011), *The Protection and Security of Electronic Information Held By Australian Government Agencies*.

[1575] Advocacy groups

Do privacy advocacy groups and civil liberties groups matter? From a practitioner perspective there is disagreement. That disagreement is evident for example in comments that bodies such as the Australian Privacy Foundation (APF)[19] and Electronic Freedoms

Job: research/pic/allvols/serv_0/back_263013
Page: **14** Date: **18/8/2011** Time: **10:50:28**
bwpageid:: 14::
bwservice::0::

Australia (EFA)[20] are sometimes noisy but are unrepresentative, are largely disregarded by government (because they are extreme and lack wide community support) and in contrast to overseas counterparts such as EPIC and the EFF have not launched effective litigation.

Disagreement also reflects perceptions that the groups emulate their US peers, construing privacy in terms of intrusions by the state into the private lives of individuals and failing to recognise abuses by non-government bodies. That 'government is evil' stance means that they tend to oppose legitimate action by governments merely because it is being undertaken by officials.

It is true that the bodies are small and on occasion have taken credit for someone else's victory. The demise of the Australia Card for example was as much a matter of cost and disagreement within the national bureaucracy as it was effective action by the advocates. However, they are significant because they have a voice and because their spokespeople shape community perceptions by being available to the media. From a practitioner or manager perspective it is useful to be aware that the groups exist and to be able to quickly address potential problems when responding to queries by journalists whose perceptions have been shaped by the groups.

Notes

19 www.privacy.org.au.

20 www.efa.org.au.

[1600] Law Reform agencies

Law reform agencies, although often disregarded on a day by day basis, are potentially important to readers of this book because they shape the overall privacy environment through reports that are reflected in changes to statute law and in interpretation by the courts. If you are advising a major corporate client about likely privacy law 5 years ahead (and thus about directions for the client's information infrastructure and operational protocols) it is for example worth studying the reports from the Australian Law Reform Commission (ALRC).

The ALRC, with a national focus, is the premier law reform specialist. It has produced major reports (eg multi-volume studies of several hundred pages based on extensive community consultation) regarding privacy law reform *per se* and regarding specific areas such as genetic privacy.[21] Those reports are typically reflected in Commonwealth statute law after a lag of between five and ten years but may be apparent in guidelines or standards, such as those from the National Health & Medical Research Council affecting health privacy, over a shorter period.

Practitioners should not disregard consultations and reports by the state law reform agencies, with those in NSW and Victoria being especially active over the past five years[22] and affecting state/territory law in both the relevant jurisdiction and — through emulation — in other jurisdictions. That is potentially an issue for non-government organisations that operate across multiple jurisdictions.

Finally, parliamentary committees should not be forgotten. That is both because they are instrumental in the development of statute law and because they conduct public inquiries that may attract media attention. If your client has an interest in influencing the shape of law or merely offsetting criticism by a media-savvy advocate or politician it may be worth making a submission to the relevant committee, lobbying representatives and officials or being prepared to respond to queries by journalists.

Job: research/pic/allvols/serv_0/back_263013
Page: **15** Date: **18/8/2011** Time: **10:50:28**
bwpageid:: 15::
bwservice::0::

Notes

21 See in particular Australian Law Reform Commission (2008), *For Your Information: Australian Privacy Law & Practice* (ALRC Report 108) and (2003) *Essentially Yours: The Protection of Human Genetic Information in Australia* (ALRC Report 96). Earlier significant reports include (1979) *Unfair Publication: Defamation and Privacy*, (1979) *Privacy and the Census*, (1983) *Privacy*, and (1987) *Spent Convictions*. The reports are available on the ALRC site at www.alrc.gov.au.

22 New South Wales Law Reform Commission (2009), *Invasion of Privacy* (report 120), (1997) Surveillance (1995) *Invisible Eyes: Video Surveillance in the Workplace*. Victorian Law Reform Commission (2010), *Surveillance in Public Places — Final Report* (18), with a broader coverage than indicated by the title.

[1625] Other Actors

From a practitioner or management perspective it is worth recognising a further actor: the mass media.

In contrast to North America and Europe there are few journalists with much understanding of privacy law and practice. Editorial awareness of, and interest in privacy issues is uneven. That is potentially both a danger and opportunity for legal practitioners who are advising corporate clients, representing someone whose privacy has been breached or defending someone who is allegedly responsible for a breach.

It is axiomatic that "scare stories" in the print and electronic media get attention, with managers and practitioners on occasion being exasperated because journalists have misreported the facts, haven't found the relevant law (or simply assume that there is a comprehensive statute criminalising all photography on streets and beaches) or simply misunderstand the capability of technologies such as biometric cards and RFIDs. Unfortunately consumers of that journalism may be even more naïve. Practitioners should be aware of the potential for things to go wrong (and for example assist clients in the timely production of media releases) and for shaping community perceptions through plain-language comments when approached by the media.

[1800] A threadbare patchwork?

What then, is the shape of the Australian privacy regime?

It might be described as a patchwork of rules from several jurisdictions, some of which are inconsistent and increasingly out of date. A more positive view is that it is a regime of regimes: different rules and practices in different jurisdictions and for different industries or types of information. There is no single statute or coherent body of case law that covers all the Australian jurisdictions and all areas of government, business and personal life. Although there is increasing convergence, as might be expected because digital technologies are eroding traditional jurisdictional boundaries, it is unlikely that a truly uniform regime will emerge in the near future. Practitioners will need to be aware of changes and have some sense of different areas of privacy law.

[1825] Making sense of the law

In understanding Australian law it is important to recognise that jurisdictions still matter.

Unlike company law and the Australian Consumer Law, where there is now a coherent and uniform code across the country, privacy law still has substantial jurisdictional variation. That variation is outlined below and identified in more detail in the following chapters. Depending on the type of information and type of client, the breach of concern to you and the remedy (or defence) that is best for your client, you could be covered by Commonwealth or state/territory law.

Job: research/pic/allvols/serv_0/back_263013
Page: **16** Date: **18/8/2011** Time: **10:50:28**
bwpageid:: 16::
bwservice::0::

Australian privacy law is highly sectoral, resulting in problems that have been recurrently highlighted by the Australian Law Reform Commission, the National Health & Medical Research Council, the Australian Bankers Association and other bodies. There is no single statute that comprehensively covers all industries and all uses of information. Instead privacy law comprises a patchwork, with for example broad Commonwealth law regarding privacy co-existing with state/territory statutes that are specifically concerned with workplace privacy, the regulation of private investigators, use of covert surveillance by state police officers, medical records privacy and criminal law provisions regarding unauthorised surveillance of minors and adults. Those statutes co-exist with common law protection of confidential information, where there is an emphasis on particular relationships rather than information or privacy *per se*.

As should be evident from the preceding paragraphs, privacy law in Australia is increasingly dynamic. Change reflects demands from officials, business and consumers. It also reflects emulation, with legislators copying what is taking place in other Australian jurisdictions and in overseas jurisdictions (particularly the European Union and the United States). That leapfrogging will continue as we become more closely integrated with the global information economy and as consumers and policymakers acquire a greater awareness of privacy issues. Developments such as introduction of Google StreetMaps, the establishment of the Unique Health Identifier[23] or the Tax File Number[24] and the exposure of over 70 million accounts on the Sony PlayStation network for example have arguably done more to sensitise ordinary Australians to privacy concerns than any awareness campaign run by the Commonwealth Privacy Commissioner.

Notes

23 Healthcare Identifiers Act 2010 (Cth).

24 Taxation Laws Amendment (Tax File Numbers) Act 1988 (Cth).

[1850] Commonwealth statutes

What are the Commonwealth statutes? Commonwealth law for most people is probably construed in terms of the Privacy Act 1988 (Cth). Practitioners will however recognise that the Act, although important, sits alongside a range of Commonwealth statutes that feature privacy provisions.

Some of those provisions, in for example the Archives Act 1983 (Cth), protect privacy by prohibiting unauthorised public access to personal information. Other provisions provide law enforcement and national security personnel with access to personal information (identification of individuals, surveillance of telephone calls, postal mail and email or other communications) that would otherwise be protected through the Privacy Act and other statutes.

The enactments are accompanied by the Freedom of Information Act 1982 (Cth), substantially updated in 2010,[25] which provides statutory rights of access to information (underpinning an 'open government philosophy articulated by the Office of the Australian Information Commissioner). The FOI Act features exemptions to protect information regarding individuals and information that was provided on a confidential basis.

The Privacy Act 1988 (Cth) initially covered only Commonwealth agencies. It did not extend to the private sector or state/territory government bodies. It was a belated response to comments by the Australian Law Reform Commission, legislative proposals from the Whitlam government onwards, and the 1981 OECD *Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data* (which were formally adopted by the Commonwealth Government in 1984). After a decade the Act was extended to cover major private sector bodies.[26] The extension responded to community pressure and

Job: research/pic/allvols/serv_0/back_263013
Page: **17** Date: **18/8/2011** Time: **10:50:28**
bwpageid:: 17::
bwservice::0::

reflected increasingly comprehensive privacy Directives in Europe. The Act has since been extended to provide more comprehensive coverage, now extending to smaller private sector bodies.

As of June 2011 the Act features two sets of overarching privacy principles: one for the Commonwealth public sector and one for the private sector. Parliament is considering proposals for amendment of the Act through integration of the two sets in strengthening and rationalising the Commonwealth regime. That rationalisation will not replace the other Commonwealth statutes that feature privacy provisions and is not expected to adopt all recommendations in recent Australian Law Reform Commission or Parliamentary Committee reports.

It is likely that the amended Act will eventually be replaced with a new statute that reflects both the ALRC recommendations and the current generation of European Union Privacy Directives, along with specific US provisions on for example mandatory reporting of breaches of financial databases.

Notes

25 Freedom of Information Amendment (Reform) Act 2010 (Cth).

26 In particular see the Privacy Amendment (Private Sector) Act 2000 (Cth). For the sake of reader convenience references throughout this chapter are to the 1988 statute as amended.

[1875] State/Territory statutes

State/territory privacy statutes in Australia resemble the Commonwealth model, with discrete enactments covering privacy in relation to the provision of services by state/government agencies and separate enactments covering some aspects of privacy in the private sector, principally through restriction on surveillance in the workplace, by private investigators or by voyeurs. Examples are the Workplace Privacy Act 2010 (ACT), the Information Privacy Act 2009 (Qld), Surveillance Devices Act 1999 (Vic), Crimes Act 1900 (NSW) s 574C and Police Offences Act 1935 (Tas) s 14A.

That body of law is jurisdiction specific and often highly sectoral, with the result that what is permitted or criminalised in one jurisdiction may not be covered in another. Protection under the Crimes Act 1900 (NSW) ss 91K and 91L is for example broader than under the corresponding ACT statute; the Listening Devices Act 1992 (ACT) captures audio but not video recording in contrast to jurisdictions that have dealt with unauthorised recording *per se*.

Like the Commonwealth regime, state/territory law features statutory rights of access to official information, again with protection for personal information and for information provided on a basis of confidence.[27]

Notes

27 Right to Information Act 2009 (Qld)

[1900] Common law

Somewhat to the surprise of many journalists and graduates, common law remains significant. Although there is no common law tort of privacy there is protection relating to use of information imparted in circumstances where there is a reasonable expectation of confidence. As noted above, the law of confidence is particularly significant for personal information (for example that provided to a medical practitioner by a patient in connection with health services) but extends to information that is commercial rather than narrowly personal. Broader aspects of confidentiality are outside the scope of this work; the following chapters highlight the principles and key judgments but practitioners with

Job: research/pic/allvols/serv_0/back_263013
Page: **18** Date: **18/8/2011** Time: **10:50:28**
bwpageid:: 18::
bwservice::0::

an interest in the protection of non-privacy information are directed to other works from LexisNexis Butterworths such as name of publisher's commercial confidentiality book/service.

[1925] International Agreements

Respect for privacy is an express feature of a range of international agreements, including the *Universal Declaration of Human Rights* (UDHR)[28] of 1948, the *International Covenant on Civil and Political Rights* (ICCPR)[29] of 1966 and the *United Nations Convention on the Rights of the Child* (CROC)[30] of 1989. It is also a feature of the guidelines of the Organisation for Economic Co-operation and Development 1980 *Guidelines Governing the Protection of Privacy and the Transborder Flows of Personal Data* (OECD data protection guidelines).

Adherence to those agreements is consistent with the external affairs head of power in the national Constitution, highlighted above. The agreements are pitched at the level of principle, with considerable scope for interpretation in the development of Australian statute law and in associated regulations or interpretive guidelines. There has been no successful litigation contesting Australian accession to the agreements or the constitutional basis of privacy and data protection statutes that reflect those agreements.

Arguably a series of European Union Directives tied to the *European Convention on Human Rights* (ECHR) has been more influential as benchmarks for Australian privacy and data protection law. Those Directives include the—

- 1995 *Data Protection Directive*[31] harmonising European national law and facilitating the flow of personal information within Europe;
- 2002 *Privacy Directive*,[32] concerned with privacy and electronic communications;
- 2006 *Data Retention Directive*,[33] extending the 2002 Directive and providing for mandatory retention of telecommunication traffic information.

The Directives have been reflected in formal agreement with Australia regarding the exchange of passenger information. More importantly, they have been reflected in UK statute and case law, for example the Data Protection Act 1998, which offers benchmarks for development and implementation in Australia and which has been interpreted by English courts through reference to the *European Convention on Human Rights* (ECHR) discussed below.

Notes

28 Art 12.

29 Art 17.

30 Art 16.

31 *Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data*. The Directive establishes the Article 29 Working Party, the independent EU advisory body on data protection and privacy. For an introduction see in particular Kuner C (2007), *European Data Protection Law, Corporate Compliance and Regulation* (Oxford: Oxford University Press).

32 *Directive 2002/58/EC on Privacy and Electronic Communications*.

33 *Directive 2006/24/EC on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communication Services or Public Communication Networks*.

[1950] Standards

Although there are ISO, ANSI and ASA standards regarding information infrastructure protection (ie design, maintenance and testing) there is no comprehensive Australian or

Job: research/pic/allvols/serv_0/back_263013
Page: **19** Date: **18/8/2011** Time: **10:50:28**
bwpageid:: 19::
bwservice::0::

global standard regarding privacy. That is significant if you are drafting contracts, providing strategic policy advice, defending a client or taking action on behalf of a client whose privacy has been breached.

The absence of formal standards reflects national and industry disagreement about what we mean by privacy, what value we place on particular aspects and how we measure particular harms.[34] As the introductory paragraphs of this chapter indicate, the disagreement is unlikely to go away. In providing advice practitioners would instead be wise to consider particular technical requirements and determine whether there are formal standards regarding specific technical measures such as testing of firewalls and monitoring of large-scale networked databases for intrusions.

Notes

34 For a contrary view see Bennett C (2000), 'An International Standard for Privacy Protection: Objections to the Objections'.

[2000] The Commonwealth regime

The preceding overview indicated that the Commowealth privacy regime centres on the Privacy Act 1988 (Cth), which is currently under review, and which covers both national government agencies and private sector bodies. The Act is applicable directly and through industry codes that reflect the emphasis on co-regulation and provide a level of detail that is not available in the actual statute. The Act is complemented by a wide range of separate statutes that feature provisions dealing with privacy and the protection of or authorised access to personal information/communications, for example access in connection with national security. Commonwealth law also features the protection of confidentiality; the law of confidence is evident in numerous decisions by the High Court, Federal Court and Federal Magistrates Court.

The following paragraphs outline the Commonwealth regime. Guidance about specific aspects, along with detailed pointers to cases and statutory provisions, is provided in Chs 3.1 though 3.8 of this work.

[2025] The Privacy Act

The Privacy Act 1988 originated as a measure to control the handling by Commonwealth government agencies of the personal information of Australian citizens. It was a response to expressions of concern about the proposed Australia Card, which was envisaged as a comprehensive whole-of-government services card that would strengthen the taxation system and facilitate the delivery of welfare services. It also reflected overseas developments regarding use by government and the private sector of personal data.

The Act did not establish a broad right of privacy in all contexts and did not override state/territory law regarding workplace surveillance, medical records or covert surveillance by justice personnel. In essence it was concerned with personal data collected by government agencies in the course of public administration, typically data that people were required to provide (as distinct from data that they might choose to provide to private sector organisations, for example in applying for personal finance or insurance).

In restricting official collection and use of personal data (with substantial exemption of specific agencies or for particular purposes) the Act identified 11 Information Privacy Principles (IPP), discussed in more detail in the following chapter. In essence those principles

(1) regulate each agency's collection, storage, use and disclosure of information about individuals

Job: research/pic/allvols/serv_0/back_263013
Page: **20** Date: **18/8/2011** Time: **10:50:28**
bwpageid:: 20::
bwservice::0::

(2) allow people to access agency information that is specific to the individual
(3) allow the individual to correct that information

The Privacy Amendment (Private Sector) Act 2000 (Cth), in effect from 21 December 2001, extended the 1988 statute to cover private sector organisations. That extension initially covered only large entities; it has subsequently encompassed smaller organisations. Regulation of non-government bodies involves National Privacy Principles (NPP) that are similar to the IPP for Commonwealth agencies. Those principles are articulated in the Act, which thus features discrete NPP and IPP. They are discussed in more detail in the following chapter and specific guidance is provided in the second half of this service.

Amendment of the Privacy Act, currently underway, features a rationalisation of the Act to provide a single and coherent set of principles that is concerned with privacy per se and thus does not embody a two-tier structure in which expectations about private sector data handling are lower than handling by the Commonwealth government.

[2050] Other Acts

The 1988 Act (as amended) coexists with and refers to a range of discrete Commonwealth statutes that relate to law enforcement, national security and public administration. Areas of coverage include the population and housing census, the Public Service Act 1999 (Cth) and Defence Force Discipline Act 1992 (Cth), the national archives, spent convictions and telecommunications interception for investigation of offences under the Crimes Act 1914 (Cth). They also include regulation of telecommunication networks, with for example offences relating to misuse of a carriage service[35] and unauthorised disclosure by internet service providers and fixed/mobile phone network operators.[36]

Practitioners should note that the Privacy Act 1988 (Cth) is not the only statute dealing with privacy and does not override other statutes. Offences regarding unauthorised disclosure of personal or other information are articulated in those other statutes, which have been used in prosecutions and are reflected in administrative guidelines. Specific issues are discussed in detail in later chapters of this book dealing with types of information and relationships.

Notes

35 For example Criminal Code Act 1995 (Cth) s 474.17.

36 Telecommunications Act 1997 (Cth) Pt 13. See also Pts 14–15 of that Act.

[2100] State and Territory regimes

The mass media, as noted above, often represent privacy as a matter of Commonwealth law. From a practitioner perspective state/territory law will often be more important than the Privacy Act 1988 (Cth). That is because much of the contact between government and citizens involves non-Commonwealth agencies, rather than the national bureaucracy. It is also because state/territory law often covers covert surveillance and other action by private sector individuals and organisations.

The state/territory legislation is uneven, with inconsistencies between the jurisdictions in conceptualisation of harms and remedies. That reflects the shape of law reform processes in particular jurisdictions (with for example a greater receptiveness to change in New South Wales, Victoria and Queensland relative to Tasmania and Western Australia). It also reflects the perceived adequacy of existing law, with the ACT for example recently establishing a new workplace privacy statute but relying on technology-specific

Job: research/pic/allvols/serv_0/back_263013
Page: **21** Date: **18/8/2011** Time: **10:50:28**
bwpageid:: 21::
bwservice::0::

legislation in dealing with unauthorised surveillance outside the workplace, so that there is a lower protection in the ACT than in NSW where the Crimes Act 1900 (NSW) has been progressively updated.[37]

Broadly the state/territory statutes fall into five categories, which should be considered by practitioners in advising organisations and representing plaintiffs/defendants. Those categories are—

(1) broad statutes covering state/territory agencies (ie a whole-of-government approach);
(2) narrower statutes covering the operation of specific agencies or types of information/relationships, notable health records, adoption records and credit reporting;
(3) broad statutes covering workplace surveillance;
(4) broad anti-discrimination and human rights statutes, for example restrictions in the Equal Opportunity Act 1995 (Vic) on misuse of sensitive personal information in connection with recruitment decisions;
(5) broad crimes statutes covering trespass, peeping and prying, offensive behaviour and other activity.

Salient statutes are identified below. The identification is not exhaustive; detailed guidance is provided in later chapters that discuss particular statutes and point to the associated case law.

New South Wales
Privacy and Personal Information Protection Act 1998 (NSW)
Health Records and Information Privacy Act 2002 (NSW)
Workplace Surveillance Act 2005 (NSW)

Queensland
Information Privacy Act 2009 (Qld)

South Australia
Listening and Surveillance Devices Act 1992 (SA)

Tasmania
Listening Devices Act 1991 (Tas)

Victoria
Information Privacy Act 2000 (Vic)
Surveillance Devices Act 1999 (Vic)
Health Records Act 2001 (Vic)

Western Australia
Surveillance Devices Act 1998 (WA)

Australian Capital Territory
Workplace Privacy Act 2010 (ACT)
Listening Devices Act 1992 (ACT)
Health Records (Access and Privacy) Act 1997 (ACT)

Northern Territory
Information Act 2002 (NT)
Surveillance Devices Act 2007 (NT)

Notes

37 For some practical implications see Arnold B (2011), 'Not officers or gentlemen: Surveillance, law and the Australian Defence Force Academy webcam incident' 7(8) *Privacy Law Bulletin*.

[2200] Overseas

In understanding the Australian regimes (and in forecasting debate about the future

Job: research/pic/allvols/serv_0/back_263013
Page: **22** Date: **18/8/2011** Time: **10:50:28**
bwpageid:: 22::
bwservice::0::

development of Australian privacy law) a point of reference is provided by law in other countries. Put simply, we can look to law in the UK, Canada and elsewhere to get a sense of what is working and what Australian legislators or advocates will be citing.

[2210] Overseas Frameworks and international obligations

Preceding paragraphs have referred to international agreements regarding privacy. From a practitioner perspective three aspects are useful to note.

The first is that although Australia is a signatory to a range of international agreements, including some such as the Universal Declaration of Human Rights that specifically enshrine privacy, the protection for privacy that is provided by those agreements remains largely aspirational. Australian courts have given some recognition to the agreements but there has not been a successful challenge to local statutes on the basis that they conflict with respect for privacy under the agreements. In the absence of a Mason-style High Court it is unlikely that Australian courts will rely on the international agreements in overturning statutes that have a national security or commercial focus.

Instead, as discussed below, the Australian legislatures are likely to embrace overseas frameworks such as the Council of Europe Cybercrime Convention, an international agreement that includes parties outside Europe and that in the eyes of some critics facilitates a major erosion of telecommunications privacy, significant because many people "live online".

A second aspect should be recognised alongside the frameworks that seek to strengthen national security. The 1950 *European Convention for the Protection of Human Rights and Fundamental Freedoms* (EHCR) is driving European privacy development, having been embraced by UK and other courts in far-reaching decisions about the constitutionality of law enforcement measures and about protection from intrusions by the mass media into the private lives of individuals. Those decisions are likely to be influential in shaping Australian community debate (with law reform bodies and legislators for example referring to litigation by colourful identity Max Mosley)[38] and may be persuasive in judicial consideration. The decisions support a reconceptualisation of privacy law. Article 1 of the ECHR declared that "everyone has the right to respect for his private and family life, his home and his correspondence". As long ago as 1976 the European Commission of Human Rights commented that for many writers:

> the right to respect 'private life' is the right to privacy, the right to live, as far as one wishes, protected from publicity . . . however, the right to respect for private life does not end there. It comprises, also, to a certain degree, the right to establish and develop relationships with other human beings, especially in the emotional field for the development and fulfillment of one's own personality.

Acceptance of that comment by Australian legislators and policymakers is at odds with the claim by Dr Bagaric quoted at the beginning of this chapter. It illustrates the extent of disagreement about what we mean by privacy at the level of principle and practice.

A third aspect, implicit in the above comments, is that Australia is a party to bilateral and multilateral agreements concerned with terrorism, financial crime and offences relating to such matters as child pornography, people trafficking and computer hacking. Those agreements both strengthen and weaken data protection and privacy. They have been criticised by some advocates for whom 'information just wants to be free' (apparently at the expense of the personal dignity that underpins human rights) but are not necessarily erosive. A coherent international framework for data protection, implemented for example through statutes that enable extradition of people who hack public and private sector databases, is desirable and over time will be increasingly feasible. It is apparent in Australian adoption of the OECD data protection guidelines.

Job: research/pic/allvols/serv_0/back_263013
Page: **23** Date: **18/8/2011** Time: **10:50:28**
bwpageid:: 23::
bwservice::0::

Notes

38 *Mosley v News Group Newspapers Ltd* [2008] All ER (D) 322 (Jul); [2008] NLJR 1112; [2008] EMLR 679; [2008] EWHC 1777 (B). Mosley was awarded £60,000 damages plus £420,000 costs. See also Case of *Mosley v United Kingdom* (Application No 48009/08) ECHR 4th Chamber (2011) regarding a "right of notification" as the basis for an injunction to prevent publication.

[2220] National models

Until recently the development of privacy law in the United Kingdom lagged behind that in Australia, important because Australian courts referred to UK case law and because legislators considered the absence of a broad privacy statute. That has changed with implementation by the UK Information Commissioner of the Data Protection Act and a series of decisions by UK courts that protect personal life in relation to media intrusions, government action and private sector data handling.[39] Note however that UK courts in considering the balance between public versus private interests and misuse of private information (discussed in the following chapter) have not established a comprehensive tort of privacy that covers information and bodily integrity.[40]

The Information Commissioner has adopted a more privacy-positive stance than the Commonwealth Privacy Commissioner, proactively addressing breaches of the Act by public service agencies and businesses. The Act features stronger penalties than the Privacy Act 1988 (Cth); those penalties are likely to be reflected in future reforms in Australia, given recognition that current penalties for business are trivial and are for example inconsistent with the scale of penalties under the Spam Act 2003 (Cth).

Notes

39 See for example *Campbell v MGN Ltd* [2004] 2 AC 457; [2004] 2 All ER 995; (2004) 62 IPR 231; [2004] UKHL 22.

40 *Wainwright v Home Office* [2004] 2 AC 406; [2003] 4 All ER 969; [2003] 3 WLR 1137; [2003] UKHL 53 and *Douglas v Hello! Ltd* [2000] All ER (D) 2435; (2000) 9 BHRC 543; [2001] QB 967; [2001] 3 LRC 756.

[2230] New Zealand

Human rights in New Zealand are framed through reference to the non-justiciable Bill of Rights Act 1990 (NZ). In contrast to Australia and the UK, the New Zealand Supreme Court in *Hosking v Runting* has recently moved beyond the Privacy Act 1993 (NZ) in recognising privacy as a common law cause of action.[41] The common law tort has two elements. The first is the existence of facts for which there is a reasonable expectation of privacy. The second is whether an objective reasonable person, in considering publicity given to those facts, would find it to be highly or substantially offensive.

Notes

41 *Hosking v Runting* (2004) 7 HRNZ 301; [2005] 1 NZLR 1.

[2240] Canada and USA

Another point of reference is provided by privacy law in Canada and the United States. Both illustrate variations across sectors and jurisdictions, with Canada tying its regimes to its national human rights Charter and going further than Australia in judicial recognition of privacy as a fundamental right.

The US is interesting because national legislation such as the 1996 federal *Health Insurance Portability & Accountability Act* (HIPAA) is increasingly reflecting strong privacy or data protection statutes in leading states such as California. That legislation

Job: research/pic/allvols/serv_0/back_263013
Page: **24** Date: **18/8/2011** Time: **10:50:28**
bwpageid:: 24::
bwservice::0::

features measures that are likely to be influential in Australia, such as mandatory reporting of data breaches regarding financial information (note that the reporting is to affected individuals and regulators but is only concerned with financial data) and protection of medical information. US regulators such as the Federal Trade Commission have also been prepared to seek or impose penalties. In 2006 for example ChoicePoint agreed to pay US$15 million to settle FTC charges that its security and record-handling procedures violated consumers' privacy rights. The charges followed sale of the personal financial information of 145,000 consumers to criminals purporting to be legitimate businesses. There has been no penalty on that scale in Australia.

The US regimes are extremely uneven but are significant because they shape expectations among parts of the Australian information technology community (through for example protocols articulated by US corporations with an Australian presence and through literature aimed at IT professionals).

In advising IT staff and contractors (and in developing contractors or other agreements that feature movement of personal information from Australia) it may thus be worthwhile emphasising compliance with Australian law.

[2300] What is shaping the law?

What is shaping Australian privacy law, affecting the development of legal frameworks and practice in the public and private sectors? Broadly we can see four drivers—

(1) national security and justice;
(2) consumer expectations;
(3) technology and business;
(4) a global environment.

[2310] National security and justice

Although many Australians appear to assume that they have an overarching 'right of privacy' that right is not recognised in the national Constitution or reflected in common law. It is bounded by statute and common law regarding policing and national security, with for example expectations that people will assist law enforcement personnel by providing information on request and enactments at the Commonwealth and state/territory level that authorise covert surveillance in relation to investigation of drug trafficking, fraud against the Commonwealth, child pornography, corruption of officials and so forth.

There is a tension in lawmaking about privacy. On the one hand legislators continue to move, albeit unevenly, to strengthen privacy protection by updating and extending existing statutes. On the other hand they continue to reinforce law authorising official activity that would otherwise breach that protection or imposing new requirements that are privacy-invasive. One example is legislation for Australia's accession to the Council of Europe Cybercrime Convention, with mandatory long-term retention by internet service providers and other telecommunication network operators of information about voice and fax calls, email and websurfing.[42]

We can expect the parliaments to provide the intelligence community, the police and bodies such as the NSW Independent Commission Against Corruption with tools that address challenges involving online social networks, communication technologies such as voice over internet protocol telephony (eg Skype), *hawala* banking, "drug mules", identity theft and so forth. We can also expect ongoing calls for strengthening of identity verification schemes, with for example extension of biometric databases and identity card schemes at airports, ports and other critical infrastructure. Much national security development is driven by the availability of new law enforcement technologies, so the use of body scanning, automated number plate recognition and CCTV-based biometric systems will become pervasive, eliciting challenges from privacy advocates.

Job: research/pic/allvols/serv_0/back_263013
Page: **25** Date: **18/8/2011** Time: **10:50:28**
bwpageid:: 25::
bwservice::0::

From a practitioner perspective it is useful to remember that much of the new law will be untested and open to challenge. Some will be inconsistent, badly drafted or poorly implemented.

Notes

42 See in particular Senate Environment & Communications References Committee (2011), *The Adequacy of Protections for the Privacy of Australians Online*, Keyser M (2003), 'The Council of Europe Convention on Cybercrime', 12(2) *Journal of Transnational Law & Policy* 287 and Feiler L (2010), 'The Legality of the Data Retention Directive in Light of the Fundamental Rights to Privacy and Data Protection', 1(3) *European Journal of Law and Technology* 1.

[2320] Consumer expectations

Preceding paragraphs have referred to consumer perceptions — and to the shaping of those perceptions by journalists, advocacy organisations, law reform agencies and other bodies. Those perceptions affect whether people believe that they have any rights and are in a position to enforce rights. More broadly they influence expectations about what organisations can and should do, for example provide readily intelligible privacy statements in contracts or on websites.

From a practitioner perspective the most useful advice is to be conscious that although some consumers appear to be indifferent to privacy (evident for example in behaviour online and in responses to questions by privacy researchers), some are both articulate and conscious of privacy concerns. Comprehensive data about attitudes across the Australian community is unavailable but studies by the Australian Communications & Media Authority, the Victorian Privacy Commissioner and the Commonwealth Privacy Commissioner appear to suggest that there is a growing awareness of privacy issues in general and that some areas are attracting strong concerns. Practitioners in advising clients, drafting public policy or seeking redress should be conscious that indifference cannot be taken for granted and that reputational damage may follow bad behaviour even if there is no clear legal remedy.

[2330] Technology and business

Increased privacy awareness reflects the enthusiasm with which businesses, not-for-profit entities (charities, advocacy bodies, political parties) and government agencies have embraced information technology. We can expect that embrace to continue because digital tools for low-cost collection, integration and analysis of personal information offers major advantages in relationship building and risk minimisation (for example highly targeted marketing and exclusion of poor credit risks or past offenders). Data mining is similarly attractive to law enforcement and national security personnel, reflecting both opportunities for discovery of new information and the shift of some offenders or associates to new media such as mobile phones and online social networks.

A hard-headed assessment is that the technology will not go away and is not necessarily antithetical to good privacy practice. The Unique Health Identifier, for example, offers substantial benefits for individual patients and for the Australian community as funder of the public health system. Technology does need however to be bounded by coherent privacy law. The coming decade provides opportunities and challenges for legal practitioners in advising on that law — the above listing highlights the thinness of statute law in some jurisdictions — and acting for plaintiffs/defendants in the application of specific statutes and related policies.

[2340] A global environment

It is axiomatic that Australia is part of a global information environment. That is evident in increasing integration with overseas trading partners, in decision-making by

Job: research/pic/allvols/serv_0/back_263013
Page: **26** Date: **18/8/2011** Time: **10:50:28**
bwpageid:: 26::
bwservice::0::

overseas managers with subsidiaries in Australia, and sensitivities about the offshoring of datahandling to call centres and other facilities in India, Malaysia and the Philippines. It is also evident in consideration by journalists, consumers, judicial officers and parliaments of how other jurisdictions are handling privacy. We can expect that consideration to continue and intensify, which is one reason why this book points to overseas developments rather than narrowly reporting Australian law.

[2400] Future Developments

From a practitioner perspective how is the privacy environment likely to develop in future?

The answer to that question is just a bit more complicated than predicting the next winner of the Melbourne Cup, where at least we know that a horse will come first.

Local and overseas privacy incidents (for example intrusions by journalists, such as those at the *News of the World* in the UK, and large-scale unauthorised access to computer networks, such as exposure of over 70 million accounts on the Sony PlayStation network and an undetermined number of accounts on the Vodafone Australia dealer network)[43] are likely to sensitise consumers and result in calls for greater regulation. That regulation may include mandatory reporting of data breaches, adopting the model pioneered in Californian law regarding financial and medical information.

Incidents may, however, have a counter-intuitive effect, with consumers experiencing "privacy fatigue" or "privacy defeatism": heeding Scott McNealy's comment that "your privacy has gone, so get over it" and taking less care after assuming that their data is almost certainly going to be exposed at some time. One conclusion might be that irrespective of statutory fixes, in advising clients it is important for practitioners to look ahead and to highlight potential reputational risk rather than merely the possibility of a sanction by the Privacy Commissioner or another regulator.

As of June 2011 there are no indications that a large-scale class action over privacy breaches in Australia will be successful and penalties imposed by local regulators (in contrast to their overseas peers) continue to be small.

Notes

43 Arnold B (2011), 'Leaky Databases: Law and Data Loss at Sony, 7(9) *Privacy Law Bulletin*.

[2410] Privacy-Invasive Technologies and social media

We can assume that many consumers will continue to embrace technologies and services, such as Facebook, that are privacy-invasive. Emerging issues include the regulation of biometric tools, particularly automated face recognition on the internet (initially through the leading social network services but extending beyond that to the range of publicly-accessible online photographs) and perimeter controls (for example finger, palm and retina readers in workplaces, health and educational institutions). Those issues also include increasingly pervasive use of geospatial identification technologies, with for example tagging of vehicles, communications and transactions on a time-and-location basis. Uptake of privacy facilitation tools such as P3P is likely to remain low, given the lack of regulatory incentives and very weak support from industry.

[2420] Globalisation

Law in the European Union, evident in the *von Hannover*[44] and *Mosley*[45] decisions, is heading towards greater protection of the private life of celebrities and by extension of ordinary people. That development is likely to be influential in Australian public policy debate and in specific proposals for law reform. The strengthening of the European data

Job: research/pic/allvols/serv_0/back_263013
Page: **27** Date: **18/8/2011** Time: **10:50:28**
bwpageid:: 27::
bwservice::0::

protection Directives, which are progressively becoming more comprehensive and sophisticated, is also likely to be influential. One driver of statutory development in Australia is likely to be EU impatience over Australian compliance with the Directives, relevant in movement of information across national borders.

Notes

44 *von Hannover v Germany* (2004) 16 BHRC 545; [2004] EMLR 379.

45 *Mosley v News Group Newspapers* [2008] All ER (D) 322 (Jul); [2008] NLJR 1112; [2008] EMLR 679; [2008] EWHC 1777 (B).

[2430] New Frontiers

Some privacy analysts, such as the author of this chapter, have suggested that in developing effective privacy regimes we need to emphasise principles rather than particular technologies, types of information, relationships or interactions. That emphasis addresses the emergence of new technologies and new policy conundrums, that have typically not been quickly addressed by lawmaking on a reactive basis. The tendency of privacy law to play "catch-up", with for example discrete statutes dealing with particular sectors, responding to outrages or belatedly adopting recommendations made by a law reform agency in a previous decade means that privacy protection continues to be uncertain and uneven.

Genetic privacy represents one such new frontier, with for example potential problems in genetic sorting within Australia and the emergence of direct-to-consumer genetic testing services that operate from overseas.

[2440] New Freedoms?

Irrespective of the fate of Julian Assange (in court as this work went to press) the "open information" philosophy of Wikileaks and its competitors will pose a challenge for practitioners who are concerned with data protection and privacy. Wikileaks under-values or simply disregards privacy and confidentiality, illustrated by Assange's willingness to publish account details of bank customers and impatience with deleting the names of informants. The idea that "secrecy" or "confidentiality"is necessarily bad should be a concern for any practitioner who is concerned with the rule of law (some matters are properly dealt with by courts rather than in Wikipedia or Facebook or the *Australian Financial Review*). It should also be of concern to information managers and practitioners advising executives about the law of confidentiality.

Australian law has limited scope for retrieving information once a personal file, customer list, medical report or financial database has left the building in someone's briefcase, on a USB or via an email. In an environment where people seek to emulate Assange it is important for practitioners to remind clients/colleagues of traditional confidentiality mechanisms. Mark files as confidential. Include confidentiality statements in the start-up screens of corporate networks. Familiarise staff and contractors with confidentiality policies. Enforce those policies rather than assuming that people will be conscientious.

[2450] A tort of privacy?

Will Australia establish a broad tort of privacy? The answer to that question is unclear. Establishment through statute has been suggested by the NSW Law Reform Commission, the Victorian Law Reform Commission and the Australian Law Reform Commission but as of June 2011 there has been no action by any of the legislatures.

Job: research/pic/allvols/serv_0/back_263013
Page: **28** Date: **18/8/2011** Time: **10:50:28**
bwpageid:: 28::
bwservice::0::

The ALRC suggested a cause of action for serious invasion of privacy, including protection of a plaintiff's right to seclusion (eg in a bedroom) in circumstances where claimants have reasonable expectations of privacy and the defendants' acts or conduct are highly offensive to a reasonable person of ordinary sensibilities. Proof of actual damage (economic or physical harm) would not be required. Remedies would include ordinary and aggravated damages, injunction, apology, a correction order and an account of profits.[46]

The Victorian report called for creation of two new statutory causes of action dealing with serious invasions. After noting that the act of intruding upon a person's seclusion or invading their private space is in itself objectionable conduct, irrespective of any publication, it recommended overlapping causes of action that would address the difficulty jurists' face in conceptualising privacy. One cause would cover misuse of private information (including dissemination of images). The second would deal with invasion of a person's seclusion, in particular through use of a surveillance device to monitor conduct that a person reasonably believes to be private or view parts of a person not open to public gaze.[47]

The NSW report did not restrict the tort to serious invasions of privacy.[48]

A New Zealand-style personal tort is unlikely to emerge, if ever, until after passage of the amendments to the Privacy Act 1988 (Cth) that are currently in train. A broad tort would substantially change the landscape and it is likely that the High Court, which has not ruled out tort protection, would be concerned to restrict the scope of protection.

Notes

46 Australian Law Reform Commission (2008), *For Your Information: Australian Privacy Law & Practice — Final Report vol 3* (ALRC Report 108) recommendation 74.

47 Victorian Law Reform Commission (2010), *Surveillance in Public Places: Final Report* 150.

48 New South Wales Law Reform Commission (2009), *Invasion of Privacy* (NSWLRC Report 120) 4.11.

[2500] Other sources of information

The dynamic nature of privacy and data protection law in Australia and overseas means that updating of any practitioner guide or academic reference work is an ongoing task. An excellent source of up-to-date information about recent and future developments is *Privacy Law Bulletin*, the companion publication to this service.

Privacy Law Bulletin is published 10 times a year. It is aimed at legal practitioners and other privacy or data protection specialists. It features news and commentary on—

- recent cases;
- proposed legislation;
- developments overseas with a direct impact on the Australian regimes;
- books and official reports of particular importance;
- legal aspects of events such as large-scale data loss at Sony and the ADFA webcam incident.

It is written by senior practitioners and academics, with an editorial board chaired by former High Court Justice Michael Kirby and including senior legal counsel and privacy officials.

Job: research/pic/allvols/serv_0/back_263013
Page: **29** Date: **18/8/2011** Time: **10:50:28**
bwpageid:: 29::
bwservice::0::

Job: research/pic/allvols/serv_0/back_263013
Page: **30** Date: **18/8/2011** Time: **10:50:28**
bwpageid:: 30::
bwservice::0::