Australia Privacy Laws (detailed)

Wikipedia, the free encyclopedia

http://en.wikipedia.org/wiki/Privacy_in_Australian_law December 08, 2014

What is privacy? There is no statutory definition of privacy in Australia. The (ALRC) was given a reference to review Australian privacy law in 2006.

Privacy in Australian law is the right of natural persons to protect their personal life from invasion and to control the flow of their personal information. Privacy is not an absolute right; it differs in different contexts and is balanced against other competing rights and duties. It is affected by the Australian common law and a range of Commonwealth, State and Territorial laws and administrative arrangements.[1]

Looking across the Tasman, the New Zealand Law Commission said in 2009:

"The current landscape in Australia includes Federal and state information privacy legislation, some sector-specific privacy legislation at state level, regulation of the media and some criminal sanctions. Regarding civil causes of action for invasion of privacy, however, the current position in Australia is unclear. There have been some indications by the courts that a tort of invasion of privacy may exist in Australia. The Australian Law Reform Commission has recommended the enactment of a statutory cause of action for invasion of privacy."[2]:para 4.87

There is no statutory definition of privacy in Australia.[1] The Australian Law Reform Commission (ALRC) was given a reference to review Australian privacy law in 2006. During that review it considered the definition of privacy in 2007 in its Discussion paper 72. The ALRC found that there is no "precise definition of universal application" of privacy; instead it conducted the inquiry considering the contextual use of the term "privacy".[3]:para 1.37-1.45

In reaching that conclusion, the ALRC began by considering the concept of privacy:[3]:para 1.29

It is unclear if a tort of invasion of privacy exists under Australian law. The ALRC summarised the position in 2007:[3]:para 5.12, 5.14

"In Australia, no jurisdiction has enshrined in legislation a cause of action for invasion of privacy; however, the door to the development of such a cause of action at common law has been left open by the High Court in Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd (Lenah Game Meats). To date, two lower courts have held that such a cause of action is part of the common law of Australia. ..."

"At common law, the major obstacle to the recognition in Australia of a right to privacy was, before 2001, the 1937 High Court decision in Victoria Park Racing and Recreation Grounds Co Ltd v Taylor (Victoria Park). In a subsequent decision, the High Court in Lenah Game Meats indicated clearly that the decision in Victoria Park 'does not stand in the path of the development of … a cause of action (for invasion of privacy)'. The elements of such a cause of action — and whether the cause of action is to be left to the common law tradition of incremental development or provided for in legislation — remain open questions."

Australian Privacy Foundation

http://www.privacy.org.au/Resources/PLawsCth.html December 08, 2014

Introduction. This document provides access to Australian laws relevant to privacy, and to many resources that point to yet more laws. Please advise us of ...

This document is a partner to pages on Privacy Laws of the Australian States and Territories, on Privacy Laws of the World and on International Instruments

This document provides access to Australian laws relevant to privacy, and to many resources that point to yet more laws. Please advise us of improvements that should be made. The links in this page are reviewed periodically. Please advise any broken links to the APF Web-Team.

The remainder of this document presents Commonwealth laws, which are relevant throughout the country. If you are looking for the laws of a State or Territory, those details are in another document. See: N.S.W., Victoria, Queensland, Western Australia, South Australia, Tasmania, A.C.T., Northern Territory.

This page contains the following sections:

The primary statute is the Privacy Act 1988. The original version applied to the Commonwealth public sector. It was amended in 1990 to apply also to the credit reporting industry. It was then further amended in 2000 to apply to much of the private sector. The original statute was adequate, the 1990 credit reporting amendment reasonably strong, and the 2000 private sector amendment so bad that some people thought that it was the world's worst privacy legislation. Subsequently, the NSW Act challenged it for that mantle. But then the 2012 amendments were passed, which make the Privacy Act (Cth) unequivocally the most privacy-hostile data protection law in the world.

The law has all manner of exceptions, exemptions, authorisations and designed-in loopholes scattered through it, and the complexities are such that there are many unintended loopholes, ambiguities and uncertainities as well. Corporations and expensive lawyers and consultants spend a lot of time wading through the verbiage in order to find multiple ways in which organisations can breach data privacy, but not data privacy law.

The statute is here:

The Attorney-General's Department's ComLaw database can also be used, by searching on 'Privacy Act', and then sifting through the hundreds of hits to find the particular document and version that you want.

The Privacy Act granted the National Health and Medical Research Council the extraordinary power to issue its own guidelines. For these, see:

The Spam Act 2003 came into effect on 10 April 2004. Under the new law it is illegal to send, or cause to be sent, 'unsolicited commercial electronic messages' that have an Australian link. The Australian Communications Authority enforces the Spam Act, and provides information about spam laws and spam security, and means for reporting spam.

There is a vast array of legislation that authorises surveillance by Commonwealth agencies, much of it enacted since September 2001, most of it grossly excessive, and most of it subject to seriously inadequate controls. Valuable summaries are provided by the Commonwealth Parliamentary Library, but they keep disappearing every few years, because web-site re-designs are conducted with a cavalier attitude to history, and information policy standards in government seem to be non-existent, or else seriously inadequate. The latest round of searching, in November 2013, found the following:

As an apparently necessary precaution, APF has provided a mirror of the version of October 2007.

A statute of particular relevance is:

The Privacy Commissioner's site states that the Health Insurance Commission and the federal Department of Health and Family Services are bound

by the Medicare and Pharmaceutical Benefits Programs privacy guidelines.

The Privacy Act granted the National Health and Medical Research Council the extraordinary power to issue its own guidelines. For these, see:

In Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd (2002) 208 CLR 199, a majority of the High Court held that Australian courts were not prevented from finding that there is a tort (or legal cause of action) of unjustified invasion of privacy. But they did not find that it existed on the facts of the case before them, and no other significant sign of life has ever been seen.

See also the ALRC's Recommendation of a Privacy Cause of Action ALRC (2008b).

The Office of the Federal Privacy Commissioner's Guide to Privacy Laws in Australia

The Office of the Federal Privacy Commissioner's Guide to State Privacy Laws

Two papers on history and issues, Clarke (1998a-) and Clarke (1998b-)

AMCRAN (2004) 'Terrorism Laws: ASIO, the Police and You', 2004, Australian Muslim Civil Rights Advocacy Network, July 2004, at http://www.amcran.org/booklet/TerrorLawsV1.html

Wikipedia, the free encyclopedia

http://en.wikipedia.org/wiki/Privacy_law December 08, 2014

The current state of privacy law in Australia includes Federal and state information privacy legislation, some sector-specific privacy legislation at state level ...

Privacy law refers to the laws which deal with the regulation of personal information about individuals which can be collected by governments and other public as well as private organizations and its storage and use.

Privacy laws are considered in the context of an individual's privacy rights or reasonable expectation of privacy.

Privacy laws can be broadly classified into:

Article 8 of the European Convention on Human Rights, which was drafted and adopted by the Council of Europe in 1950 and meanwhile covers the whole European continent except for Belarus and Kosovo, protects the right to respect for private life: "Everyone has the right to respect for his private and family life, his home and his correspondence." Through the huge case-law of the European Court of Human Rights in Strasbourg, privacy has been defined and its protection has been established as a positive right of everyone.

Article 17 of the International Covenant on Civil and Political Rights of the United Nations of 1966 also protects privacy: "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

The current state of privacy law in Australia includes Federal and state information privacy legislation, some sector-specific privacy legislation at state level, regulation of the media and some criminal sanctions. The current position concerning civil causes of action for invasion of privacy is unclear: some courts have indicated that a tort of invasion of privacy may exist in Australia; in 2008, the Australian Law Reform Commission recommended the enactment of a statutory cause of action for invasion of privacy.[1]

A Brazilian citizen's privacy is protected by the country's constitution, which states:

In Canada, the federal Personal Information Protection and Electronic Documents Act (PIPEDA) governs the collection, use and disclosure of personal information in connection with commercial activities and personal information about employees of federal works, undertakings and businesses. It generally does not apply to non-commercial organizations or provincial governments. Personal information collected, used and disclosed by the federal government and many crown corporations is governed by the Privacy Act. Many provinces have enacted similar provincial legislation such as the Ontario Freedom of Information and Protection of Privacy Act which applies to public bodies in that province.

There remains some debate whether there exists a common law tort for breach of privacy. There have been a number of cases identifying a common law right to privacy but the requirements have not been articulated.[3]

In Eastmond v. Canadian Pacific Railway & Privacy Commissioner of Canada[4] Canada's Supreme Court found that CP could collect Eastmond's personal information without his knowledge or consent because it benefited from the exemption in paragraph 7(1)(b) of PIPEDA, which provides that personal information can be collected without consent if "it is reasonable to expect that the collection with the knowledge or consent of the individual would compromise the availability or the accuracy of the information and the collection is reasonable for purposes related to investigating a breach of an agreement".[4]

Computer Processed Personal Information Protection Act was enacted in 1995 in order to protect personal information processed by computers. The general provision specified the purpose of the law, defined crucial terms, prohibited individuals from waiving certain rights.

Two Greek laws relevant to privacy are 57 AK and 2472/1997. As regarding photography:

India has no dedicated privacy [7] and data protection laws [8] and the same has been interpreted by Indian Supreme Court in Article 21 of the Indian Constitution. India is also weak at protecting civil liberties in cyberspace.[9] A parliamentary committee also slammed Indian government for poor privacy laws in India.[10]

Some legal experts have reiterated that privacy is a human right that Indian government cannot deny.[11] Like other countries, India is also using national security as an excuse to invade privacy of Indian citizens.[12] The demands to ensure privacy rights in India has significantly increased in the recent days.[13]

In June, 2011, India passed a new privacy package that included various new rules that apply to companies and consumers. A key aspect of the new rules requires that any organization that processes personal information must obtain written consent from the data subjects before undertaking certain activities. Application of the rule is still uncertain.[14]

Previously, the Information Technology (Amendment) Act, 2008 made changes to the Information Technology Act, 2000 and added the following two sections relating to Privacy:

Section 43A, which deals with implementation of reasonable security practices for sensitive personal data or information and provides for the compensation of the person affected by wrongful loss or wrongful gain.[15]

Section 72A, which provides for imprisonment for a period up to 3 years and/or a fine up to Rs. 5,00,000 for a person who causes wrongful loss or wrongful gain by disclosing personal information of another person while providing services under the terms of lawful contract.[15]

In July 5, 2010, Mexico passed a new privacy package focused on treatment of personal data by private entities. The key elements included where:

In New Zealand, the Privacy Act 1993 sets out principles in relation to the collection, use, disclosure, security and access to personal information.

The introduction into the New Zealand common law of a tort covering invasion of personal privacy at least by public disclosure of private facts was at issue in Hosking v Runting.

Complaints about privacy are considered by the Privacy Commissioner

As a general rule, consent of the individual is required for processing, i.e. obtaining, organizing, accumulating, holding, adjusting (updating, modifying), using, disclosing (including transfer), impersonating, blocking or destroying of his personal data. This rule doesn't apply where such processing is necessary for performance of the contract, to which an individual is a party.

As a member of the European Convention on Human Rights, the United Kingdom adheres to Article 8 ECHR, which guarantees a "right to respect for privacy and family life" from state parties, subject to restrictions as prescribed by law and necessary in a democratic society towards a legitimate aim.

However, there is no independent tort law doctrine which recognises a right to privacy. This has been confirmed on a number of occasions.

The right to privacy is not explicitly stated anywhere in the Bill of Rights. The idea of a right to privacy was first addressed within a legal context in the United States. Louis Brandeis (later a Supreme Court justice) and another young lawyer, Samuel D. Warren, published an article called "The Right to Privacy" in the Harvard Law Review in 1890 arguing that the U.S. Constitution and common law allowed for the deduction of a general "right to privacy".[16]

Their project was never entirely successful, and the renowned tort expert Dean Prosser argued that "privacy" was composed of four separate torts, the only unifying element of which was a (vague) "right to be left alone".[17] The four torts were:

For additional information on Privacy laws in the United States, see:

Though the right to privacy exists in several regulations, the most effective privacy protections come in the form of constitutional articles of Uzbekistan. Varying aspects of the right to privacy are protected in different ways by different situations.

States and Territories

http://www.privacy.org.au/Resources/PLawsST.html December 08, 2014

Introduction. This document provides access to Australian laws relevant to privacy, and to many resources that point to yet more laws. Australia is a federation of 6 ...

This document is a partner to pages on Privacy Laws of the Australian Commonwealth, on Other Countries' Privacy Laws and on International Instruments

This document provides access to Australian laws relevant to privacy, and to many resources that point to yet more laws. Australia is a federation of 6 States and 2 Territories. This document is concerned with laws of those 8 jurisdictions. A separate document provides access to laws that are relevant throughout the country.

Please advise us of improvements that should be made. The links in this page are reviewed periodically. Please advise any broken links to the APF Web-Team.

The remainder of this document presents laws of the States and Territories of Australia, as follows:

The Office of the Federal Privacy Commissioner provides a Guide to State Privacy Laws, which may help orient you to what follows.

The Office of the Victorian Privacy Commissioner provides a comprehensive list of Privacy & Related Legislation in Australia.

Two papers on history and issues, Clarke (1998a-) and Clarke (1998b-)

Data Protection Laws in Australia

https://www.efa.org.au/Issues/Privacy/privacy.html December 08, 2014

Electronic Frontiers Australia (EFA) pages providing information about Australian data protection / privacy legislation.

Australian privacy laws are contained in a variety of Commonwealth, State and Territory Acts. The "Privacy Acts" are data protection laws which regulate the collection, use and disclosure of personal information about individuals; they do not protect privacy of the individual in a broader sense. In relation to use of the Internet and other telecommunications services, ISPs and telephone service providers are also required to comply with the privacy protection provisions of the Telecommunications Act 1997 (C'th) and the Telecommunications (Interception) Act 1979 (C'th). A variety of other legislation contains privacy protection provisions relevant to particular types of entities and/or practices, for example, the Spam Act, surveillance and listening devices acts, and many others.

The remainder of this page provides information about the Privacy Acts. For information about other privacy laws relevant to use of the Internet and other telecommunications systems, refer to the topic listing on EFA's Privacy and Surveillance Page.

The Privacy Act 1988 applied to Commonwealth and A.C.T. government entities and credit reporting organisations until December 2001. Since then, it has also applied to other private sector organisations.

The Privacy Amendment (Private Sector) Act 2000 (C'th) amended the Privacy Act 1988 to regulate some, but not all, private sector organisations/businesses. It was passed by Parliament in December 2000 and became operative on 21 December 2001 (some provisions did not commence until 21 December 2002).

The Act includes ten National Privacy Principles (NPPs) regulating the collection, use and disclosure of personal information by private sector organisations. The Parliament chose to leave 'flexibility' (which in context is a synonym for ambiguity) in the NPPs, and the legislation empowers the Federal Privacy Commissioner to make guidelines in relation to interpretation of the NPPs. The Commissioner's interpretation of the ambiguous aspects of the NPPs is crucial to the extent of protection of individuals' privacy provided by the legislation, at least in the first instance and the development of the guidelines in 2001 was controversial.

The Federal Privacy Commissioner is also empowered to investigate and resolve complaints made by individuals against organisations that have not complied with the NPPs, including making a formal determination. However, the Act does not provide complainants with a right of appeal against a determination of the Commissioner. It does, however, in effect provide a right of appeal to organisations complained about. If the Commissioner interprets the NPPs and law in a manner that finds a breach by the organisation, the organisation can simply refuse to comply and wait to see if the Commissioner or the complainant seek to have the Federal Court or the Federal Magistrates Court order the organisation to

comply. As a Court must hear the matter anew, in effect the organisation obtains a right of appeal. However, if the Commissioner interprets the law in a non-privacy protective manner and the complainant considers the Commissioner's application of the law to the facts of their case is questionable, the complainant has no means of appeal. (There is no requirement that the Commissioner even be a lawyer.

During the Bill's second reading speech (on 12 April 2000), the then Attorney-General Daryl Williams said that "a formal review of the operation of the legislation, and of all the exemptions, in consultation with key stakeholders" would be conducted "after it has been in operation for 2 years". However, the review of the Act did not commence until over 2.5 years later (in August 2004 with a reporting date of 31 March 2005) and a number of the exemptions were specifically excluded from the review's terms of reference. In December 2004 the Senate Legal and Constitutional References Committee commenced an Inquiry into the Privacy Act 1988 with terms of reference significantly broader than the governmental review. Further information about the 2004/05 reviews is provided below in the section titled Parliamentary & Government Agency Inquiries.

The Commonwealth Privacy Act does not apply to State/Territory government agencies (except for the A.C.T.)

Some State and Territory Parliaments have enacted privacy legislation applicable to their own government agencies/departments and some of those laws also apply to private sector organisations.

For more information see the State Privacy Laws page on the Federal Privacy Commissioner's web site which includes links to State/Territory privacy laws/regulations and to State/Territory Privacy Commissioners' web sites.

In December 2004 the Senate Legal and Constitutional References Committee commenced an Inquiry into the Privacy Act 1988 with a reporting date of 30 June 2005.

This review was undertaken by the Federal Privacy Commissioner at the request of the Federal Attorney General.

In July 2000, the Senate Select Committee on Information Technologies announced an Inquiry into ePrivacy. EFA prepared a submission to the inquiry and was invited to appear at the Committee's hearing in Canberra on 21st August 2000.

Two parliamentary inquiries were conducted into the above Bill during 2000. EFA sent written submissions to both inquiries and also presented oral testimony at the House Committee's hearing:

In April 2000, the Attorney General tabled the Privacy Amendment (Private Sector) Bill 2000, claiming it to be a "light touch" co-regulatory regime. The Bill was drafted as an amendment to the Privacy Act 1988. Unfortunately the Bill was riddled with exemptions for direct marketing, small business, the media and political parties, and contained weak enforcement provisions. EFA and other privacy advocates considered that the Bill was unlikely to meet the requirements of the European Data Protection Directive, thus potentially jeopardising opportunities for Australia to take its place in the global information economy. While EFA supports fair privacy legislation, EFA considered the Bill pandered to business interests and was a totally inadequate response by the government to this important issue.

In May 2000, the Federal Government referred the Privacy Amendment (Private Sector) Bill 2000 to the House Standing Committee on Legal and Constitutional Affairs for inquiry and report. EFA made a submission to the Inquiry and presented oral testimony at one of the Committee's hearings. The Committee's report was tabled in Parliament on 26 June 2000. The report made a number of positive recommendations to improve the legislation, but did not go far enough in addressing major deficiencies in the Bill.

In September 2000, the corresponding Senate Committee undertook its own inquiry, but the majority government report made only minor recommendations.

The Bill, with minor amendments, was eventually passed into law in December 2000 and became operative on 21 December 2001. (Some provisions did not commence until twelve months later on 21 December 2002).

In early 2001, the then Federal Privacy Commissioner (Malcolm Crompton) convened an NPP Guidelines Reference Group consisting of representatives from business, consumer, etc. groups (including EFA), to assist his office in developing guidelines. In May 2001, the Commissioner released draft NPP Guidelines for public consultation with a submission closure date of 6 July 2001. The introductory section stated:

EFA lodged a submission that was generally supportive of the contents of the public consultation draft, and also addressed a number of areas where the guidelines could be made clearer or otherwise improved.

On 14 August 2001, a further meeting of the NPP Reference Group was held and the Commissioner invited a number of people who had not been prior participants, the majority representing business groups.

Seven days later (21 Aug), an article on the Sydney Morning Herald's Breaking News web page reported that:

On 24 August 2001, the Federal Attorney General issued a media release which stated inter-alia:

On the same day (24 Aug), the Federal Privacy Commissioner distributed a substantially revised draft of the guidelines to the NPP Reference Group and, apparently, unnamed others. This draft was provided to the NPP Reference Group for comment on condition of confidentiality of the contents. Regrettably, EFA is therefore unable to publish the draft or EFA's specific comments thereon. However, on 31 August 2001, EFA issued an open letter to the Commissioner expressing general disapproval of the contents of the (non-public) revised draft and stating, among other things, that:

On 18 September 2001, final Guidelines on the National Privacy Principles were made publicly available by the Privacy Commissioner. These are a slightly amended version of the non-public draft referred to in EFA's open letter and the minor amendments are insufficient to change EFA's previously expressed views.

In addition to the Guidelines, the Privacy Commissioner issued a number of supplementary Information Sheets. It is concerning, however, that the Commissioner decided not to issue all previously planned Information Sheets and those that disappeared would have covered important, albeit controversial, issues such as Consent.

In 1997 an Australian coalition of privacy rights, commerce and academic groups commenced a campaign for fair privacy laws. Subsequently, Commonwealth legislation applicable to the private sector became operative in December 2001 although it contains many loopholes and inadequacies. See separate page for information about the campaign, campaign documents and related privacy reference materials.

Australia Cloud Data Privacy Laws

http://perspecsys.com/how-we-help/cloud-privacy/australia-data-privacy-laws/ December 08, 2014

Laws in Australia and New Zealand make it difficult to move sensitive information to cloud-providers outside of their borders. PerspecSys has a solution.

According to the October 2012 Cloud Computing in Australia Market Report from IBIS World, the Australian cloud industry has incredible growth potential. Demand is expected to be driven by the tremendous benefits it brings enterprises, including lower costs, enhanced speed of information sharing, and the rapid development & delivery of new capabilities. In Australia, 2012 total industry revenue is expected to be $1.24 billion, up 7.8% on the previous year.

But while this growth is impressive, it trails the growth being experienced by other regions around the globe. One factor frequently cited to explain why many Australian organizations have been slow to adopt cloud services is related to jurisdictional control of data that is moved offshore to the U.S. and other foreign countries. The concern is that Australian data stored in datacenters overseas will be subject to International laws that are less stringent than the laws at home that safeguard individual and corporate privacy. Whether or not courts outside of Australia have jurisdiction in cases such as this is a legal issue that has not yet been settled, but in a whitepaper by global law firm Freshfields, Bruckhaus Deringer, it was highlighted that, “Within Australia, government, community and industry concern around data privacy is growing. The current federal government has expressed particular concern about the potential exposure of personal data once it is transferred offshore.”

Regulations in Australia and New Zealand make it extremely difficult for enterprises to move sensitive information to cloud-providers that store data outside of Australian/New Zealand borders. The Office of the Australian Information Commissioner (OAIC) is chartered with providing oversight on data privacy regulations designed to govern the dissemination of sensitive personal information (PII, Medical Records, etc.). One example of the type of legislation they enforce is the The Australian National Privacy Act of 1988, which regulates how organizations collect, use, keep, secure, and disclose personal information. The National Privacy Principles (NPP) set out in the Act were designed to ensure that organizations holding personal information about people handle it responsibly, especially health service providers.

The NPP cover the process of collection, use, disclosure, access, correction and identification of any personal information. They state, “An organization must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.” They also require enterprises to put very rigorous security Service-level Agreements (SLAs) in place with their cloud service providers that define audit rights, reporting, data location constraints, and access right provisions when cross-border disclosure of personal information are involved (i.e. data leaves Australian/New Zealand borders).

The Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Privacy Amendment Act) was passed in late 2012.

The Privacy Amendment Act introduces many significant changes to the Privacy Act effective March 2014. The Privacy Amendment Act includes a set of new privacy principles that will regulate the handling of personal information by both Australian government agencies and businesses. These new principles are called the Australian Privacy Principles (s). They will replace the existing Information Privacy Principles ( ) that currently apply to Australian Government agencies and the National Privacy Principles ( ) that currently apply to businesses.

In the context of Cloud, agencies and businesses that deal with personal information need to be mindful that:

Source: DLA Piper Australia: Cloud computing and the new Australian privacy law

Under the APP privacy, security and regulatory issues related to the use of cloud services must be managed and addressed in agreements.

Financial Services organizations, in particular, are subject to very stringent cloud restrictions. The Australian Prudential Regulatory Authority (APRA) oversees the Financial services vertical and has stated that financial services companies that wish to transfer data offshore must first notify APRA and demonstrate to the regulator that the cloud service provider has put appropriate risk management procedures in place to protect sensitive data. Enterprises must also secure guarantees in their contracts with offshore data hosting companies that APRA will have access to hosting facilities in order to conduct site visits at their discretion. In the context of the global Cloud, where the third-party provider is likely to be using a number of data centres in different countries (both primary and disaster recovery sites) and have employees from multiple jurisdictions with access to Australian data, these requirements have been difficult-to-impossible to meet. Cloud service providers have simply been reluctant to sign-up to the strong guarantees around data security that enterprises need in order to satisfy APRA.

A good resource is the Data Sovereignty and the Cloud – A Board and Executive Officer’s Guide. This white paper by David Vaile, Kevin Kalinich, Patrick Fair and Adrian Lawrence outlines the technical, legal and risk governance issues around data hosting and jurisdiction.

The AppProtex Cloud Data Protection Gateway lets Australian enterprises define their data protection policies to ensure that sensitive data is appropriately secured and protected in cloud applications. Authorized data security administrators can select, on a field-by-field basis, whether to allow a data going to the cloud to remain in clear text, to be encrypted, or to be replaced with a token. When using tokens as a surrogate value, sensitive data never leaves the organization’s control in any format – making it particularly useful for organizations that need to adhere with Australia’s National Privacy Principles.

The data in the cloud is either tokenized or encrypted so it is meaningless when viewed in the cloud, and organizations can be confident that their sensitive data is within their full control at all times.

Learn more about how Perspecsys helps enterprises meet data residency/sovereignty requirements from around the globe including in China, Canada and Switzerland.

Download our whitepaper International Privacy Laws, which speaks to various laws and how to meet them.

Australian health information and privacy laws

http://www.mondaq.com/australia/x/271204/data+protection/Australian+health+information+and+privacy+laws December 08, 2014

Australia privacy rights are regulated by Commonwealth and State legislation and the laws protecting confidential information under the common law.

Mondaq.com (the Website) is owned and managed by Mondaq Ltd and as a user you are granted a non-exclusive, revocable license to access the Website under its terms and conditions of use. Your use of the Website constitutes your agreement to the following terms and conditions of use. Mondaq Ltd may terminate your use of the Website if you are in breach of these terms and conditions or if Mondaq Ltd decides to terminate your license of use for whatever reason.

You may use the Website but are required to register as a user if you wish to read the full text of the content and articles available (the Content). You may not modify, publish, transmit, transfer or sell, reproduce, create derivative works from, distribute, perform, link, display, or in any way exploit any of the Content, in whole or in part, except as expressly permitted in these terms & conditions or with the prior written consent of Mondaq Ltd. You may not use electronic or other means to extract details or information about Mondaq.coms content, users or contributors in order to offer them any services or products which compete directly or indirectly with Mondaq Ltds services and products.

Mondaq Ltd and/or its respective suppliers make no representations about the suitability of the information contained in the documents and related graphics published on this server for any purpose. All such documents and related graphics are provided "as is" without warranty of any kind. Mondaq Ltd and/or its respective suppliers hereby disclaim all warranties and conditions with regard to this information, including all implied warranties and conditions of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Mondaq Ltd and/or its respective suppliers be liable for any special, indirect or consequential damages or any damages whatsoever resulting from loss of use, data or profits, whether in an action of contract, negligence or other tortious action, arising out of or in connection with the use or performance of information available from this server.

The documents and related graphics published on this server could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Mondaq Ltd and/or its respective suppliers may make improvements and/or changes in the product(s) and/or the program(s) described herein at any time.

Mondaq Ltd requires you to register and provide information that personally identifies you, including what sort of information you are interested in, for three primary purposes:

Mondaq (and its affiliate sites) do not sell or provide your details to third parties other than information providers. The reason we provide our information providers with this information is so that they can measure the response their articles are receiving and provide you with information about their products and services.

If you do not want us to provide your name and email address you may opt out by clicking here .

If you do not wish to receive any future announcements of products and services offered by Mondaq by clicking here .

We require site users to register with Mondaq (and its affiliate sites) to view the free information on the site. We also collect information from our users at several different points on the websites: this is so that we can customise the sites according to individual usage, provide 'session-aware' functionality, and ensure that content is acquired and developed appropriately. This gives us an overall picture of our user profiles, which in turn shows to our Editorial Contributors the type of person they are reaching by posting articles on Mondaq (and its affiliate sites) meaning more free content for registered users.

We are only able to provide the material on the Mondaq (and its affiliate sites) site free to site visitors because we can pass on information about the pages that users are viewing and the personal information users provide to us (e.g. email addresses) to reputable contributing firms such as law firms who author those pages. We do not sell or rent information to anyone else other than the authors of those pages, who may change from time to time. Should you wish us not to disclose your details to any of these parties, please tick the box above or tick the box marked "Opt out of Registration Information Disclosure" on the Your Profile page. We and our author organisations may only contact you via email or other means if you allow us to do so. Users can opt out of contact when they register on the site, or send an email to unsubscribe@mondaq.com with no disclosure in the subject heading

In order to receive Mondaq News Alerts, users have to complete a separate registration form. This is a personalised service where users choose regions and topics of interest and we send it only to those users who have requested it. Users can stop receiving these Alerts by going to the Mondaq News Alerts page and deselecting all interest areas. In the same way users can amend their personal preferences to add or remove subject areas.

A cookie is a small text file written to a users hard drive that contains an identifying user number. The cookies do not contain any personal information about users. We use the cookie so users do not have to log in every time they use the service and the cookie will automatically expire if you do not visit the Mondaq website (or its affiliate sites) for 12 months. We also use the cookie to personalise a user's experience of the site (for example to show information specific to a user's region). As the Mondaq sites are fully personalised and cookies are essential to its core technology the site will function unpredictably with browsers that do not support cookies - or where cookies are disabled (in these circumstances we advise you to attempt to locate the information you require elsewhere on the web). However if you are concerned about the presence of a Mondaq cookie on your machine you can also choose to expire the cookie immediately (remove it) by selecting the 'Log Off' menu option as the last thing you do when you use the site.

Some of our business partners may use cookies on our site (for example, advertisers). However, we have no access to or control over these cookies and we are not aware of any at present that do so.

We use IP addresses to analyse trends, administer the site, track movement, and gather broad demographic information for aggregate use. IP addresses are not linked to personally identifiable information.

This web site contains links to other sites. Please be aware that Mondaq (or its affiliate sites) are not responsible for the privacy practices of such other sites. We encourage our users to be aware when they leave our site and to read the privacy statements of these third party sites. This privacy statement applies solely to information collected by this Web site.

From time-to-time our site requests information from users via surveys or contests. Participation in these surveys or contests is completely voluntary and the user therefore has a choice whether or not to disclose any information requested. Information requested may include contact information (such as name and delivery address), and demographic information (such as postcode, age level). Contact information will be used to notify the winners and award prizes. Survey information will be used for purposes of monitoring or improving the functionality of the site.

If a user elects to use our referral service for informing a friend about our site, we ask them for the friends name and email address. Mondaq stores this information and may contact the friend to invite them to register with Mondaq, but they will not be contacted more than once. The friend may contact Mondaq to request the removal of this information from our database.

This website takes every reasonable precaution to protect our users information. When users submit sensitive information via the website, your information is protected using firewalls and other security technology. If you have any questions about the security at our website, you can send an email to webmaster@mondaq.com.

If a users personally identifiable information changes (such as postcode), or if a user no longer desires our service, we will endeavour to provide a way to correct, update or remove that users personal data provided to us. This can usually be done at the Your Profile page or by sending an email to EditorialAdvisor@mondaq.com.

If we decide to change our Terms & Conditions or Privacy Policy, we will post those changes on our site so our users are always aware of what information we collect, how we use it, and under what circumstances, if any, we disclose it. If at any point we decide to use personally identifiable information in a manner different from that stated at the time it was collected, we will notify users by way of an email. Users will have a choice as to whether or not we use their information in this different manner. We will use information in accordance with the privacy policy under which the information was collected.

You can contact us with comments or queries at enquiries@mondaq.com.

If for some reason you believe Mondaq Ltd. has not adhered to these principles, please notify us by e-mail at problems@mondaq.com and we will use commercially reasonable efforts to determine and correct the problem promptly.

Australia Privacy Law

http://lawbrain.com/wiki/Australia_Privacy_Law December 08, 2014

Australian privacy law is concerned with the protection and preservation of the privacy rights of its citizens.

It's a living legal community making laws accessible and interactive. Click Here to get Started »

Australian privacy law is concerned with the protection and preservation of the privacy rights of its citizens.

Australian privacy laws follow a co-regulatory approach whereby industry develops privacy and data protection standards which are enforced by both the industry and a privacy agency.

The National Privacy Principles (NPPs)[1] are standards related to personal information held by certain private sector organizations. These organizations must comply with these principles, especially all health service providers in the private sector.

The National Privacy Principles were taken from the Privacy Act of 1988. These principles include:

The Information Privacy Principles (IPPs)[2] regulate how Australian and Australian Capital Territory (ACT) (a self-governing territory) government agencies manage personal information. Specifically, how and when personal information can be collected, used, disclosed, stored and secured.

The Information Privacy Principles were taken from Section 14 of the Privacy Act of 1988. These principles include:

The Privacy Act covers the handling of personal information by both private sector and government entities. It limits how personal information is collected, used, disclosed to third-parties and secured. Additionally, the information must be accuarate and access must be given to individuals so that they can make changes to any errors. This act follows basic fair information practices.

The Privacy Act does not regulate state or territory agencies, except for the Australian Capital Territory (ACT).

Oversight: Office of the New South Wales Privacy Commissioner

Oversight: Office of the Information Commissioner for the Northern Territory[13]

Australia Cheap Credit & Australia Privacy Laws

http://www.streetdirectory.com/travel_guide/161940/credit_matters/australia_cheap_credit__australia_privacy_laws.html December 08, 2014

While Australia's privacy laws are currently being reviewed, it is unlikely the latest proposals put forward by those in charge of the country's privacy system will ...

The reason that Australian consumers have to pay more for their credit than their northern hemisphere cousins is that the Australian privacy system prevents lenders sharing with each other the type of information that would improve their ability to spot the people who are likely to fail to make their repayments.

Most lenders use a credit scoring system to decide who to lend money to. Credit scoring is a mathematical formula, which uses a consumer's credit history and lifestyle to predict how likely a potential customer is to repay their debt.

Because lenders in Australia cannot share consumers' credit payment performance information with the credit reference agencies, as they can in the UK and US, it is much harder for Australian lenders to weed out the people who are most likely to fail to make their repayments. As a result Australian lenders tend to charge higher interest rates to cover the cost of lending money to people who fail to repay.

In the UK and US the cost of credit is relatively cheap because lenders are able to access the credit payment performance information of potential customers. Lenders are able to keep bad debt levels to a minimum and are able to avoid having to pass on the extra cost of bad debt to their customers.

The type of information that Australian lenders are currently permitted to share with the credit reference agencies for credit checking purposes includes records of when customers are 60 days late with their payments, and information to help verify consumers' identities.

Most lenders have called for Australian law to be changed to allow them to share a wider range of credit information, including how good consumers are at meeting their monthly payments. Lenders say they would be better able to identify those consumers struggling to meet their debts, which would allow them to reduce the price they charge for

Privacy campaigners fear that a loosening of Australian financial privacy rules may lead to an increase in the amount of credit available to consumers. They are also concerned this could lead to a hike in the numbers of people facing financial meltdown.

The Australian Law Reform Commission, which is responsible for putting forward suggested changes to Australian privacy laws, is currently against increasing the range of permitted credit information made available to lenders to the levels permitted in the UK and US.

For Australian consumers the price for maintaining strong financial privacy is likely to be felt most keenly in their wallets. While Australia's privacy laws are currently being reviewed, it is unlikely the latest proposals put forward by those in charge of the country's privacy system will help give Australians access to cheaper credit.The reason that Australian consumers have to pay more for their credit than their northern hemisphere cousins is that the Australian privacy system prevents lenders sharing with each other the type of information that would improve their ability to spot the people who are likely to fail to make their repayments.Most lenders use a credit scoring system to decide who to lend money to. Credit scoring is a mathematical formula, which uses a consumer's credit history and lifestyle to predict how likely a potential customer is to repay their debt.Because lenders in Australia cannot share consumers' credit payment performance information with the credit reference agencies, as they can in the UK and US, it is much harder for Australian lenders to weed out the people who are most likely to fail to make their repayments. As a result Australian lenders tend to charge higher interest rates to cover the cost of lending money to people who fail to repay.In the UK and US the cost of credit is relatively cheap because lenders are able to access the credit payment performance information of potential customers. Lenders are able to keep bad debt levels to a minimum and are able to avoid having to pass on the extra cost of bad debt to their customers.The type of information that Australian lenders are currently permitted to share with the credit reference agencies for credit checking purposes includes records of when customers are 60 days late with their payments, and information to help verify consumers' identities.Most lenders have called for Australian law to be changed to allow them to share a wider range of credit information, including how good consumers are at meeting their monthly payments. Lenders say they would be better able to identify those consumers struggling to meet their debts, which would allow them to reduce the price they charge for credit.Privacy campaigners fear that a loosening of Australian financial privacy rules may lead to an increase in the amount of credit available to consumers. They are also concerned this could lead to a hike in the numbers of people facing financial meltdown.The Australian Law Reform Commission, which is responsible for putting forward suggested changes to Australian privacy laws, is currently against increasing the range of permitted credit information made available to lenders to the levels permitted in the UK and US.For Australian consumers the price for maintaining strong financial privacy is likely to be felt most keenly in their wallets.

Users Reading this article are also interested in;

About The Author, Tristan Dunston

Tristan Dunstan is an independent public relations consultant specialising in finance and privacy matters. He loves white water canoeing and photography.

Privacy Laws

http://www.lawyers.com.au/legal-articles/privacy-laws-australia/ December 08, 2014

Did you know that Australia has no legal definition for privacy

Did you know that Australia has no legal definition for privacy? When the Australian Law Reform Commission (ALRC) reviewed Australian privacy law back in 2007, it determined that there was "no precise decision of universal application" of privacy.

Because of this, the ALRC looked into the use of the term "privacy". Here's what they concluded regarding the concept of privacy:

The lack of statutory definition of privacy is probably one of the major reasons why the debate has dragged on for a while. In recent years, however, the argument heated up when ALRC recommended a statutory cause of action to justify having a tort for invasion of privacy.

Reaction to ALRC's proposal has been varied. Peter Bartlett of The Australian, for instance, disagrees with the report because of its "failure to adequately protect freedom of speech". In the case Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd, then-Chief Justice Murray Gleeson noted that there's no clear distinction between what's private and what's not.

And speaking of free speech, Australia doesn't have constitutional protection of free speech, so a tort for invasion of privacy could conflict with that issue. In fact, media lawyers like Justin Quill warned The Australian that current privacy legislation could influence free speech.

"Privacy can be as wide as you want it to be," said Quill. "Even if this is never used, its mere existence will have a chilling effect and will lead to news editors taking out facts from stories for fear of being sued," he said.

Quill's concerns are echoed Nic Pullen, another media lawyer, who was concerned because the proposal will make it "impossible" to define privacy with no legal uncertainty, which could be used by the government as a defence for the media when keeping away privacy lawsuits.

But until the line between private and public is clearly delineated, the debate will continue. Of course, it's nice to have a clear, well-defined policy on privacy, which is an important human right, but we think free speech and freedom of information holds a bit more weight in the scales of justice.

Privacy Laws In Australia

http://www.youthcentral.vic.gov.au/know-your-rights/privacy December 08, 2014

Youth Central looks at the importance of privacy, the laws that protect people's privacy in Victoria, and what you can do to protect your privacy.

Organisations are required by law to protect the privacy of your personal information. Three laws help protect Victorians' privacy:

The Information Privacy Act covers the way State government organisations, statutory bodies and local councils collect and handle your personal information.

It contains 10 Information Privacy Principles (new window). With some exceptions, all Victorian government organisations, including local councils, must observe these principles. Non-government organisations that work for government under contract may also be covered.

The principles, in simple terms, state that when an organisation collects personal information that it should:

Privacy Victoria, the Office of the Victorian Privacy Commissioner, regulates the way that the Victorian government and local councils collect and handle personal information. It is an independent statutory office created by the Information Privacy Act. Its goal is to get privacy better understood and respected, inside and outside the Victorian public sector.

You can find lots more info about privacy at the Privacy Victoria website (new window).

'Personal information' means recorded information or opinions, whether true or not, about an identifiable person. Personal information can be almost any information linked to someone, including:

If you believe an organisation that holds your personal information has breached your privacy, firstly you should try to resolve the matter with them.

Ask to speak to the privacy officer or someone who deals with complaints. Write to the organisation, explaining the situation and what you would like to see happen. Give the organisation time to respond.

If you are still not satisfied, you have the right to complain to the Privacy Commissioner (new window). The Commissioner will try to solve your problem.

If a solution to the problem is not reasonably possible or if an attempt at a solution fails, your complaints may go to the Victorian Civil and Administrative Appeals Tribunal (VCAT), the official body for complaint and dispute resolution in Victoria.

If you win your dispute because the organisation is found to have not followed one or more of the Information Privacy Principles, they might have to:

There are other organisations in Australia that protect your privacy within other jurisdictions.

Privacy Victoria

Privacy Victoria regulates the way that the Victorian government and local councils collect and handle personal information. If you have a complaint about the way your personal information has been handles, you can register a complaint with them.

Victorian Civil and Administrative Appeals Tribunal (VCAT)

VCAT is a low cost, accessible and independent dispute resolution tribunal available to all Victorians.

Privacy Law in Australia: The Status Quo

http://www.mondaq.com/australia/x/67038/Data+Protection+Privacy/Privacy+Law+in+Australia+The+Status+Quo December 08, 2014

Traditionally Australian law has not recognised any general "right to privacy". A number of existing areas of law deal with different aspects of what might ...

Mondaq.com (the Website) is owned and managed by Mondaq Ltd and as a user you are granted a non-exclusive, revocable license to access the Website under its terms and conditions of use. Your use of the Website constitutes your agreement to the following terms and conditions of use. Mondaq Ltd may terminate your use of the Website if you are in breach of these terms and conditions or if Mondaq Ltd decides to terminate your license of use for whatever reason.

You may use the Website but are required to register as a user if you wish to read the full text of the content and articles available (the Content). You may not modify, publish, transmit, transfer or sell, reproduce, create derivative works from, distribute, perform, link, display, or in any way exploit any of the Content, in whole or in part, except as expressly permitted in these terms & conditions or with the prior written consent of Mondaq Ltd. You may not use electronic or other means to extract details or information about Mondaq.coms content, users or contributors in order to offer them any services or products which compete directly or indirectly with Mondaq Ltds services and products.

Mondaq Ltd and/or its respective suppliers make no representations about the suitability of the information contained in the documents and related graphics published on this server for any purpose. All such documents and related graphics are provided "as is" without warranty of any kind. Mondaq Ltd and/or its respective suppliers hereby disclaim all warranties and conditions with regard to this information, including all implied

warranties and conditions of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Mondaq Ltd and/or its respective suppliers be liable for any special, indirect or consequential damages or any damages whatsoever resulting from loss of use, data or profits, whether in an action of contract, negligence or other tortious action, arising out of or in connection with the use or performance of information available from this server.

The documents and related graphics published on this server could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Mondaq Ltd and/or its respective suppliers may make improvements and/or changes in the product(s) and/or the program(s) described herein at any time.

Mondaq Ltd requires you to register and provide information that personally identifies you, including what sort of information you are interested in, for three primary purposes:

Mondaq (and its affiliate sites) do not sell or provide your details to third parties other than information providers. The reason we provide our information providers with this information is so that they can measure the response their articles are receiving and provide you with information about their products and services.

If you do not want us to provide your name and email address you may opt out by clicking here .

If you do not wish to receive any future announcements of products and services offered by Mondaq by clicking here .

We require site users to register with Mondaq (and its affiliate sites) to view the free information on the site. We also collect information from our users at several different points on the websites: this is so that we can customise the sites according to individual usage, provide 'session-aware' functionality, and ensure that content is acquired and developed appropriately. This gives us an overall picture of our user profiles, which in turn shows to our Editorial Contributors the type of person they are reaching by posting articles on Mondaq (and its affiliate sites) meaning more free content for registered users.

We are only able to provide the material on the Mondaq (and its affiliate sites) site free to site visitors because we can pass on information about the pages that users are viewing and the personal information users provide to us (e.g. email addresses) to reputable contributing firms such as law firms who author those pages. We do not sell or rent information to anyone else other than the authors of those pages, who may change from time to time. Should you wish us not to disclose your details to any of these parties, please tick the box above or tick the box marked "Opt out of Registration Information Disclosure" on the Your Profile page. We and our author organisations may only contact you via email or other means if you allow us to do so. Users can opt out of contact when they register on the site, or send an email to unsubscribe@mondaq.com with no disclosure in the subject heading

In order to receive Mondaq News Alerts, users have to complete a separate registration form. This is a personalised service where users choose regions and topics of interest and we send it only to those users who have requested it. Users can stop receiving these Alerts by going to the Mondaq News Alerts page and deselecting all interest areas. In the same way users can amend their personal preferences to add or remove subject areas.

A cookie is a small text file written to a users hard drive that contains an identifying user number. The cookies do not contain any personal information about users. We use the cookie so users do not have to log in every time they use the service and the cookie will automatically expire if you do not visit the Mondaq website (or its affiliate sites) for 12 months. We also use the cookie to personalise a user's experience of the site (for example to show information specific to a user's region). As the Mondaq sites are fully personalised and cookies are essential to its core technology the site will function unpredictably with browsers that do not support cookies - or where cookies are disabled (in these circumstances we advise you to attempt to locate the information you require elsewhere on the web). However if you are concerned about the presence of a Mondaq cookie on your machine you can also choose to expire the cookie immediately (remove it) by selecting the 'Log Off' menu option as the last thing you do when you use the site.

Some of our business partners may use cookies on our site (for example, advertisers). However, we have no access to or control over these cookies and we are not aware of any at present that do so.

We use IP addresses to analyse trends, administer the site, track movement, and gather broad demographic information for aggregate use. IP addresses are not linked to personally identifiable information.

This web site contains links to other sites. Please be aware that Mondaq (or its affiliate sites) are not responsible for the privacy practices of such other sites. We encourage our users to be aware when they leave our site and to read the privacy statements of these third party sites. This privacy statement applies solely to information collected by this Web site.

From time-to-time our site requests information from users via surveys or contests. Participation in these surveys or contests is completely voluntary and the user therefore has a choice whether or not to disclose any information requested. Information requested may include contact information (such as name and delivery address), and demographic information (such as postcode, age level). Contact information will be used to notify the winners and award prizes. Survey information will be used for purposes of monitoring or improving the functionality of the site.

If a user elects to use our referral service for informing a friend about our site, we ask them for the friends name and email address. Mondaq stores this information and may contact the friend to invite them to register with Mondaq, but they will not be contacted more than once. The friend may contact Mondaq to request the removal of this information from our database.

This website takes every reasonable precaution to protect our users information. When users submit sensitive information via the website, your information is protected using firewalls and other security technology. If you have any questions about the security at our website, you can send an email to webmaster@mondaq.com.

If a users personally identifiable information changes (such as postcode), or if a user no longer desires our service, we will endeavour to provide a way to correct, update or remove that users personal data provided to us. This can usually be done at the Your Profile page or by sending an email to EditorialAdvisor@mondaq.com.

If we decide to change our Terms & Conditions or Privacy Policy, we will post those changes on our site so our users are always aware of what information we collect, how we use it, and under what circumstances, if any, we disclose it. If at any point we decide to use personally identifiable information in a manner different from that stated at the time it was collected, we will notify users by way of an email. Users will have a choice as to whether or not we use their information in this different manner. We will use information in accordance with the privacy policy under which the information was collected.

You can contact us with comments or queries at enquiries@mondaq.com.

If for some reason you believe Mondaq Ltd. has not adhered to these principles, please notify us by e-mail at problems@mondaq.com and we will use commercially reasonable efforts to determine and correct the problem promptly.

Workplace Privacy Laws in Australia

http://www.lawyers.com.au/legal-articles/workplace-privacy-laws-in-australia/ December 08, 2014

Here are some of the issues surrounding workplace privacy in Australia.

The term "privacy" is defined as the state where one isn't observed or disturbed by other people. It also involves the freedom from public attention and keeping personal information confidential. Therefore, workplace privacy refers to the rights of employees to privacy.

This sounds straightforward enough, but when placed in the context of business, which needs to quantify productivity in the workplace, the issue can sometimes become contentious. Business owners naturally want to monitor their staff, limit liability and deter questionable activity (or inactivity). As a result, employees need to relinquish some of their privacy. The question is how much privacy should be relinquished?

The absence of a statutory definition of privacy in Australia compounds the matter. There are a number of laws that deal with privacy, but according to a 2007 review by the Australian Law Reform Commission or ALRC, there is currently no accurate definition of its universal use.

There is, however, the Privacy Act, which was implemented in 1988 to regulate information privacy. The Privacy Act contains ten National Privacy Principles or NPPs that govern the collection, management, and use of personal data. The NPPs are applicable to some small businesses, health service providers, non-government organisations, and private businesses that have a yearly turnover of at least $3 million.

In response to the ALRC's review, the Privacy Amendment (Enhancing Privacy Protection) Act 2012, otherwise known as the Privacy Amendment Act, was passed with amendments on November that year. The act will bring a number of important changes to the 1988 law. This would include the following:

The amendments will be implemented starting March 2014.

The dispute concerning workplace privacy usually starts because of different expectations. A company, for instance, may provide its workers with a laptop, smartphone, e-mail address, office, and network access through a username and password, which may be changed every so often for better security. All of these gives workers the mistaken impression of privacy, and that no one else can access what the employer provided.

Unfortunately, some employees fail to understand that the company has the right to access your files in its computer network, even if it's password-protected. This includes your internet browsing history and e-mail messages.

To avoid conflict and clarify expectations, businesses should set expectations about workplace privacy. This should at least include the following:

According to the Fair Work Ombudsman, since businesses have access to sensitive personal data about its workers, they have to think about the way they collect, use, and disclose the data. Federal privacy laws are only applicable to employee personal information if the data is used for something not directly related to the professional employer-worker relationship.

As for dealing with employee personal information, companies need to say when they intend to gather the data, why they are collecting it, and who they plan to give it to. Businesses should also allow its workers to access their own personal data so that they can check if it is outdated, incomplete, or inaccurate.

Take note that certain states and territories have their own laws regarding workplace privacy. To find out more, consult your corresponding state body about your privacy concerns.

Australia must rewrite privacy laws for the Information Age

http://www.alrc.gov.au/news-media/privacy/australia-must-rewrite-privacy-laws-information-age December 08, 2014

The Australian Law Reform Commission’s landmark report For Your Information: Australian Privacy Law and Practice (ALRC 108), was launched today in Sydney by the ...

The Australian Law Reform Commission’s landmark report For Your Information: Australian Privacy Law and Practice (ALRC 108), was launched today in Sydney by the Cabinet Secretary, the Hon Senator John Faulkner, and the Attorney-General, the Hon Robert McClelland MP. The three-volume, 2700 page report is the culmination of a massive research and consultation exercise conducted over two years, and recommends 295 changes to privacy laws and practices.

ALRC President, Professor David Weisbrot, said that “Although the federal Privacy Act is only 20 years old, it was introduced before the advent of supercomputers, the Internet, mobile phones, digital cameras, e-commerce, sophisticated surveillance devices and social networking websites—all of which challenge our capacity to safeguard our sensitive personal information.

“The Privacy Act has worked pretty well to date, but it now needs a host of refinements to help us navigate the Information Superhighway. These days, information privacy touches almost every aspect of our daily lives, including our medical records and health status, our finances and creditworthiness, the personal details collected and stored on a multiplicity of public and corporate databases, and even the ability to control the display and distribution of our own images.”

Commissioner in charge of the Privacy Inquiry, Professor Les McCrimmon, added that “During our extensive consultations around the country, the overwhelming message we heard was that Australians do care about privacy, and they want a simple, workable system that provides effective solutions and protections.

At the same time, people appreciate that other interests often come into the balance—such as freedom of speech, child protection, law enforcement and national security. Australians also want the considerable benefits of the Information Age, such as shopping and banking online, and communicating instantaneously with friends and family around the world. And, of course, businesses want to be able to market effectively to current and potential customers, and to process data efficiently—including offshore.

Professor Weisbrot noted that “the ALRC was given many examples of the Privacy Act being used inappropriately as a reason for failing to provide information or assistance. Privacy regulators refer to this as ‘the BOTPA’ excuse, for ‘Because of the Privacy Act’. This underlines the pressing need for simplification and harmonisation of law and practice, as well as more education about what the law does—and does not—require.

“In For Your Information, the ALRC provides a clear framework for establishing world’s best practice in privacy protection. The massive range of issues has resulted in a huge report—but really this report comprises eight or nine substantial inquiries in one.

“A one-size-fits-all approach could never work, so we have endeavoured to craft sensible solutions to the various particular problems. In many cases, this will involve the Privacy Commissioner providing education and guidance to individuals, businesses and government agencies, but in other circumstances, stronger action and sanctions may be required.”

The key recommendations in the For Your Information report include:

Australian Privacy Laws and Health Information

http://holmanwebb.com.au/publications/privacy-law-reform-and-health-information December 08, 2014

Australian Privacy Laws and Health Information. Author: Alison Choy Flannigan, Partner October 2013 Australia privacy rights are regulated by Commonwealth and State ...

Author: Alison Choy Flannigan, Partner

October 2013

Australia privacy rights are regulated by Commonwealth and State legislation and the laws protecting confidential information under the common law.

Australian privacy laws govern the collection, use and disclosure of “personal information”. Further, individuals are provided with a right of access and correction of their own personal information. There are also data security, data quality and cross-border transborder data flow requirements.

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

In Australia, health information (such as medical records) are a subset of personal information and attract additional protection and rules. These include:

- Use and disclosure is permitted if there is a serious and imminent threat to the health and safety of an individual or the public.
- Use and disclosure for health and medical research if certain conditions are met.
- Disclosures to carers for compassionate reasons.
- Restrictions on access if providing direct access would pose a serious threat to the life or health of any individual.
- Use and disclosure of genetic information to lessen or prevent a serious threat to a genetic relative.

(a) information or an opinion about:

(i) the health or a disability (at any time) of an individual; or

(ii) an individual’s expressed wishes about the future provision of health services to him or her; or

(iii) a health service provided, or to be provided, to an individual; that is also personal information; or

(b) other personal information collected to provide, or in providing, a health service; or

(c) other personal information about an individual collected in connection with the donation, or intended donation, by the individual of his or her body parts, organs or body substances; or

(d) genetic information about an individual in a form that is, or could be, predictive of the health of the individual or a genetic relative of the individual.

(a) an activity performed in relation to an individual that is intended or claimed (expressly or otherwise) by the individual or the person performing it:

(i) to assess, record, maintain or improve the individual’s health; or

(ii) to diagnose the individual’s illness or disability; or

(iii) to treat the individual’s illness or disability or suspected illness or disability; or

(b) the dispensing on prescription of a drug or medicinal preparation by a pharmacist.

The Privacy Act 1988 (Commonwealth) (Privacy Act), which applies to Australian Commonwealth government agencies and private sector organisations, has been recently amended by the Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth) (Privacy Amendment Act). The Privacy Amendment Act was passed by Parliament on 29 November 2012, received the Royal Assent on 12 December 2012 and comes into force on 12 March 2014.

- Create a single set of Australian Privacy Principles applying to both Australian Government agencies and the private sector. These principles will replace the existing Information Privacy Principles and National Privacy Principles.
- Introduce more comprehensive credit reporting, improved privacy protections and more logical, consistent and simple language.
- Strengthen the functions and powers of the Australian Information Commissioner to resolve complaints, use external dispute resolution services, conduct investigations and promote compliance- penalties of up to 2000 penalty units $340K for individuals – x 5 for body corporates AUD$1.7 million.
- Create new provisions on privacy codes and the credit reporting code, including codes that will be binding on specified agencies and organisations.

The Privacy Amendment Act introduces a unified set of Australian Privacy Principles which apply to both Commonwealth agencies and the Australian private sector, replacing separate public and private sector principles.

The Privacy Amendment Act introduces the concept of “permitted health situation” in a new section 16B.

A “permitted health situation” exists in relation to the collection by an organization of health information about an individual if:(a) the information is necessary to provide a health service to the individual; and(b) either:(i) the collection is required or authorised by or under an Australian law (other than the Privacy Act); or(ii) the information is collected in accordance with rules established by competent health or medical bodies that deal withobligations of professional confidentiality which bind the organisation.

A “permitted health situation” exists in relation to the collection by an organisation of health information about an individual if:(a) the collection is necessary for any of the following purposes:(i) research relevant to public health or public safety;(ii) the compilation or analysis of statistics relevant to public health or public safety;(iii) the management, funding or monitoring of a health service; and(b) that purpose cannot be served by the collection of information about the individual that is de-identified information; and(c) it is impracticable for the organisation to obtain the individual’s consent to the collection; and(d) any of the following apply:(i) the collection is required by or under an Australian law (other than the Privacy Act);(ii)

the information is collected in accordance with rules established by competent health or medical bodies that deal withobligations of professional confidentiality which bind the organisation;(iii) the information is collected in accordance with guidelines approved under section 95A of the purposes of this subparagraph.

Use or disclosure – research, etc.

A “permitted health situation” exists in relation to the use or disclosure by an organisation of health information about an individual if:(a) the use or disclosure is necessary for research, or the compilation or analysis of statistics, relevant to public health orpublic safety; and(b) it is impracticable for the organisation to obtain the individual’s consent to the use or disclosure; and(c) the use or disclosure is conducted in accordance with guidelines approved under section 95A for the purposes this paragraph;and

(d) in the case of disclosure – the organisation reasonably believes that the recipient of the information will not disclose the

information, or personal information derived from that information.

A “permitted health situation” exists in relation to the use or disclosure by an organisation of genetic information about an individual (the first individual) if:(a) the organisation has obtained the information in the course of providing a health service to the first individual; and(b) the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to the life,health or safety of another individual who is a genetic relative of the first individual; and(c) the use or disclosure is conducted in accordance with guidelines approved under section 95AA; and(d) in the case of disclosure – the recipient of the information is a genetic relative of the first individual.

A “permitted health situation” exists in relation to the disclosure by an organisation of health information about an individual if:(a) the organisation provides a health service to the individual; and(b) the recipient of the information is a responsible person for the individual; and(c) the individual:(i) is physically or legally incapable of giving consent to the disclosure; or(ii) physically cannot communicate consent to the disclosure; and(d) another individual (the carer) providing the health service for the organisation is satisfied that either:(i) the disclosure is necessary to provide appropriate care or treatment to the individual; or(ii) the disclosure is made for compassionate reasons; and(e) the disclosure is not contrary to any wish:(i) expressed by the individual before the individual became unable to give or communicate consent;and(ii) of which the care is aware, or of which the carer could reasonably be expected to be aware; and(f) the disclosure is limited to the extent reasonable and necessary for a purpose mentioned in paragraph (d).

Please contact Alison Choy Flannigan with any questions.

This article is provided for general information purposes only and should not be relied upon as legal advice.

Privacy in Australian law

http://www.cyclopaedia.info/wiki/Privacy-in-Australian-law December 08, 2014

Privacy in Australian law is the right of natural persons to protect their personal life from invasion and to control the flow of their personal information.

Blog posts on the term

Privacy in Australian law

The Australian Government’s Privacy Amendment (Enhancing Privacy Protection) Act 2012 was enacted on 29 November 2012 but will not commence until March 2014. It contains the first significant amendments to the Privacy Act 1988 since 2001. The whole process took nearly seven years since the Australian Law Reform Commission (ALRC) started work on its privacy reform reference. This article focusses on those aspects of the law which have been changed, for better or worse. We have previously analysed the deficiencies of the Bill in articles and submissions , and the Bill was enacted with none of those deficiencies removed. The most positive aspect of the Amendment Act is the additional enforcement powers given to the Privacy Commissioner, including powers to direct remedial actions; power to make determinations following ‘own motion’ investigations; civil penalty provisions; powers to require Privacy Impact Assessments; and a new function to conduct ‘assessments’, replacing audit powers. The addition of a right of appeal to the Administrative Appeals Tribunal against determinations by the Commissioner, while very desirable, do not deal directly with the key problem of the Act: complainants cannot require the Commissoner to make determinations when they are dissatisfied with mediation and disagree with the Commissioner’s view that a complaint has been successfully resolved. Although one unified set of privacy principles in the Act is desirable, unfortunately none of the thirteen new Australian Privacy Principles (APPs) is an overall improvement, and 8 of the 13 APPs are worse for privacy protection. The most controversial new principle is APP 8, which abandons a ‘border protection’ approach in favour of ‘accountability’. The dangers of this approach are outlined. Changes to the credit report and direct marketing are also outlined.

Australian privacy law

http://www.cyclopaedia.info/wiki/Australian-privacy-law December 08, 2014

References for "Australian privacy law" online, at universities and in literature... cyclopaedia.net

The examples and perspective in this article may not represent a worldwide view of the subject. Please improve this article and discuss the issue on the talk page. (December 2010)Privacy law refers to the laws which deal with the regulation of personal information about individuals which can be collected by governments and other public as well as private organizations and its storage and use.Privacy laws are considered in the context of an individual'sor reasonable expectation of privacy This is an excerpt from the article Australian privacy law from the Wikipedia free encyclopedia. A list of authors is available at Wikipedia.

INTERNET LAW Australia Privacy Laws

http://www.ibls.com/internet_law_news_portal_view.aspx?s=latestnews&id=1856 December 08, 2014

publish a list of overseas laws and schemes which provide similar protection to Australian privacy laws, facilitating the transfer of information to those countries

The Australian Law Reform Commission (ALRC) this week released Discussion Paper 72, Review of Australian Privacy Law (discussion paper). On 31 January 2006, the Federal Government engaged the ALRC to conduct a wide-ranging review of privacy law in Australia. Click here to see our report on the ALRC's Terms of Reference. The final report of the ALRC is due to the government by 31 March 2008. The discussion paper was established primarily because of: * rapid advances in information, communication, storage, surveillance and other relevant technologies *possible changing community perceptions of privacy and the extent to which privacy should be protected by legislation

*the expansion of state and territory legislative activity in areas relevant to privacy, and

The discussion paper sets out over 300 proposals for reform of the Australian privacy framework and also asks many questions in connection with the ALRC's inquiry.

Some of the key proposals of the ALRC are set out below, grouped by subject matter.

General

introduce one set of unified privacy principles, based on the current National Privacy Principles (NPPs), to apply to all private sector organisations and the federal public sector

extend some privacy protections to the personal information of deceased persons

require that information collected is relevant to the purpose for which it was collected

remove the small business exemption

publish a list of overseas laws and schemes which provide similar protection to Australian privacy laws, facilitating the transfer of information to those countries

hold organisations liable for information sent to third parties overseas, in some circumstances

require agencies and organisations to notify individuals when there has been a data breach and there is a real risk of serious harm

empower the Privacy Commissioner to take court action to enforce its order requiring an agency or organisation to take some action within a specified timeframe

empower the Privacy Commissioner to take court action in the event of serious or repeated contravention of the law, and

develop a statutory cause of action for invasion of privacy.

Credit reporting

increase in the information that can be included in a credit reporting file to include:

type of each current credit account opened

date of opening of the current credit account

limits on each current credit account, and

date of closure of current credit account.

require credit providers to be members of an external dispute resolution scheme before they can provide default information to a credit reporting agency

remove a default listing from a credit report if a dispute in relation to that listing is not addressed within 30 days, and

enable individuals to notify credit reporting agencies of identity theft, so that the identity theft can be reported to potential credit providers.

Health

introduce one set of new health regulations to override state and territory health privacy laws as they apply to the private sector

encourage states and territories to adopt new health privacy principles for their public sectors

develop specific legislation for the regulation of an electronic health record scheme, including the treatment of unique healthcare identifiers

enable healthcare providers to collect third party personal information without that third party"s consent, if relevant and necessary, and

introduce procedures for the closure of a health service or transferring of a health service to a new owner.

Marketing

introduce a separate privacy principle addressing direct marketing in the private (and possibly public) sector:

consent required unless it is impracticable to gain consent

express consent required for sensitive information

clearly set out an opt-out regime.

Technology and telecommunications

ensure privacy laws are technologically neutral, but allow the Privacy Commissioner to develop guidelines on how to apply the Privacy Act 1988 (Cth) to particular forms of technology

consider introducing a 'take-down notice' scheme requiring a website operator to remove information that might be an invasion of an individual's privacy

prohibit charging for unlisted phone numbers, and

include email addresses and IP addresses in the definition of ‘personal information'.

Government

apply rules relating to transborder data transfer, anonymity and sensitive information to the federal public sector

encourage states and territories encouraged to adopt new unified privacy principles for their public sectors, and

remove the political exemption.

The deadline for feedback on these and the other issues raised in the discussion paper is 7 December 2007.

For further information, please visit the ALRC website.

This article was written by Kaman Tsoi, Senior Associate and Hannah Wright, Solicitor.

For more information please contact

Australian Privacy Laws

http://www.shred-x.com.au/privacy-act/ December 08, 2014

Learn about your obligations as they pertain to the new Australian Privacy Laws

The Australian Privacy Act 1988 (Cth) contains provisions that deal with:

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

sensitive information means:

(a) information or an opinion about an individual's:

(i) racial or ethnic origin; or

(ii) political opinions; or

(iii) membership of a political association; or

(iv) religious beliefs or affiliations; or

(v) philosophical beliefs; or

(vi) membership of a professional or trade association; or

(vii) membership of a trade union; or

(viii) sexual preferences or practices; or

(ix) criminal record;

that is also personal information; or

(b) health information about an individual; or

(c) genetic information about an individual that is not otherwise health information.

Australian Privacy Law states businesses must 'take reasonable steps to destroy or de-identify personal information that is no longer required.'* Not only does the careless discarding of confidential information put your business and your customer's identities at risk, you become vulnerable to significant fines.

PRIVACY, CONFIDENTIALITY 12 AND OTHER LEGAL RESPONSIBILITIES

http://www.ashm.org.au/images/publications/monographs/b%20positive/b_positive-chapter_12.pdf December 08, 2014

PRIVACY, CONFIDENTIALITY AND OTHER LEGAL RESPONSIBILITIES ... where use or disclosure is required by law. In developing Australian privacy laws, the right

PRIVACY, CONFIDENTIALITY
AND OTHER LEGAL
RESPONSIBILITIES

12

Sally Cameron Australian Federation of AIDS Organisations, NSW.

Note: This chapter refers to a number of key Australian laws and policies relating to privacy, confidentiality and duty of care, and includes a summary of significant legal cases. Although addressing some important questions, this information does not constitute legal advice. In some instances, legislation has been summarised. Practitioners faced with uncertainty in this area are strongly advised to contact their local health department, or the applicable privacy office and they ahould seek independent legal advice.

This chapter has been adapted from:
Australasian Society for HIV Medicine (ASHM). Australasian Contact Tracing Manual. Edition 3 2006. Canberra: Commonwealth of Australia, 2006: 48-51.
Available at: http://www.ashm.org.au/contact-tracing/

Links to: Chapter 11: Infection control and occupational health

Key points

- Many people are extremely sensitive about the collection and use of information related to their health and health-related treatment.
- Health care practitioners should generally only collect health information about a patient with that patient's informed consent, and should advise the patient of the potential uses of that information.
- Health care practitioners should have sophisticated systems in place governing the storage and access to health information records, including physical and technological security controls, and staff training. This is particularly important for those venues where multi-disciplinary care by different treating practitioners and allied staff may occur.
- The Privacy Act 1988 (Commonwealth) (subsequently referred to as 'the Privacy Act') is the primary piece of legislation governing the privacy of health care information in Australia. State and Territory governments also have laws and regulations affecting privacy practices, which may intersect or overlap with the Privacy Act. Health care practitioners must make themselves aware of their privacy and confidentiality obligations in their respective situations.
- Hepatitis B virus infection is a notifiable disease in every Australian State and Territory. Notification does not legally breach a patient's right to privacy, although patients should be informed that notification will occur.
- In Australia, it is illegal to discriminate against a person on the basis of their perceived hepatitis B virus infection or their perceived human immunodeficiency virus (HIV) infection.

Why is privacy and confidentiality important?

to this must be taken very seriously. They may include where there is a serious risk to the

The Australian Medical Association (AMA) Code of Ethics requires medical practitioners to maintain a patient's confidentiality. 'Exceptions patient or another person, where required by law, or where there are overwhelming societal interests.'

In Australia, the protection of health-related information has attracted special treatment, partly as a response to many people considering health information to be extremely sensitive. This point cannot be overemphasised. Most enquiries to the Office of the Privacy Commissioner are from the health sector, and the health sector is second only to the finance sector in the number of complaints received.

While the terms 'privacy' and 'confidentiality' are commonly used interchangeably, they are not identical concepts. Privacy laws regulate the handling of personal information (including health information) through enforceable privacy principles. On the other hand, the legal duty of confidentiality obliges health care practitioners to protect their patients against the inappropriate disclosure of personal (health) information.

It is important to maintain privacy and confidentiality because:

- Patients are concerned about the stigma and discrimination associated with their hepatitis B virus (HBV) status and related conditions
- Patients want to know that they can choose who has access to information about them
- Patients are far more likely to seek medical care and give full and honest accounts of their symptoms if they feel comfortable, respected and secure
- A health system with strong privacy mechanisms will promote public confidence and trust in health care services generally.

Legal requirements

There are no nationally agreed laws or guidelines specifically relating to the diagnosis, treatment and tracing of contacts of patients with HBV or other notifiable diseases. Australian States and Territories have approached the issue differently. Some jurisdictions have gone to great lengths to develop specific, targeted laws and policies, while others have relied on more generic laws and processes. (Please refer to the ashm Viral Hepatitis Models of Care database available on the ASHM website at www.ashm.org.au/hbv-moc/). However, issues relating to the management of privacy in the health sector are usually covered by the Privacy Act, which applies to all private sector organisations that provide health services and hold health information. In summary, a 'health service' can be broadly defined as including any activity that involves:

- Assessing, recording, maintaining or improving a person's health; or
- Diagnosing or treating a person's illness or disability; or
- Dispensing a prescription drug or a medicinal preparation by a pharmacist.

Consequently, health services include traditional health service providers, such as private hospitals and day surgeries, medical practitioners, pharmacists and allied health professionals, as well as complementary therapists, gyms, weight loss clinics and many others.

In general terms, the Privacy Act covers all those in the health sector (such as medical practitioners, nurses, administrators, trainers and cleaners) not directly employed by State or Territory governments (as they are usually covered by State laws). Further information on the jurisdiction of the Act is available at http://www.privacy.gov.au/publications/hg_01.html#a2.

The Privacy Act contains 10 National Privacy Principles (NPPs) (available at http://www.privacy.gov.au/publications/npps01.html), which govern the minimum privacy standards for handling personal information. Some NPPs state that health service professionals must meet certain obligations, while other NPPs require that they 'take reasonable steps' to meet stated obligations. Practitioners should familiarise themselves with the National Privacy Principles (which are legally binding), and seek advice if necessary.

The different layers of Federal, State and Territory laws and regulations do, in some instances, complicate privacy obligations. In most cases, the privacy protections required by Commonwealth and State or Territory privacy laws are similar. Under the Australian Constitution, when a State/Territory law is inconsistent with a Commonwealth law, the

12 Privacy, confidentiality and other legal responsibilities

Commonwealth law prevails. Consequently, across Australia, all private sector health service providers are required to comply with the provisions of the Commonwealth Privacy Act as well as any State/Territory laws.

In NSW, for example, State privacy legislation (the Health Records and Information Privacy Act 2002) applies to public sector, and private sector health care providers and holders of health records located in NSW. Consequently, private sector health service providers must comply with two sets of privacy legislation (Federal and NSW), which are largely, but not wholly, compatible. The two sets of legislation impose similar obligations on private health care providers. However, it could be argued that the NSW legislation has a higher compliance threshold, so that if a health care practitioner complies with the NSW Health Records and Information Privacy Act, they will generally also comply with the Federal Act (although the two sets of legislation have different enforcement regimes).

Most States now have laws severely restricting the transfer of information in the health sector, and in some States, breaches of confidentiality amount to a criminal offence. In addition to these intersecting laws, many States also have multiple layers of regulation. For example, Queensland Health's Privacy Plan points out that in addition to any relevant Commonwealth and Queensland laws, 'Queensland Health has developed a number of policies related to the management of information at Corporate Office, Directorate, District, facility and unit levels'.

A brief overview of State and Territory privacy laws (and their intersection with the Federal Privacy Act) is provided by The Office of the Privacy Commissioner at http://www.privacy.

All States obligations under the Privacy Act 1988 (Commonwealth)

The Office of the Privacy Commissioner
Tel: 1300 363 992
Email: privacy@privacy.gov.au

State and Territory specific obligations

- Australian Capital Territory
  The Office of the Privacy Commissioner
  Tel: 1300 363 992
  Email: privacy@privacy.gov.au
- New South Wales
  Privacy NSW (Office of the NSW Privacy Commissioner)
  Tel: (02) 8688 8585
  Email: privacy_nsw@agd.nsw.gov.au
- Northern Territory
  The Centre for Disease Control
  Tel: (08) 8922 8044

  The Department of Health and Community Services
  Tel: (08) 8922 7049
  Email: infoprivacy@nt.gov.au.
- Queensland
  Queensland Health
  Tel: (07) 3235 9051
  Email: privacy@health.qld.gov.au
- South Australia
  The Privacy Committee of South Australia
  Tel: (08) 8204 8786
  Email: privacy@saugov.sa.gov.au
- Tasmania
  The Office of the Ombudsman
  Tel: 1800 001 170
  Email: ombudsman@justice.tas.gov.au
- Victoria
  The Office of the Health Services Commissioner

gov.au/privacy_rights/laws/index.html#1, but for those wishing to seek specific advice (not to be confused with 'legal advice'), the following agencies can be contacted:

Tel: 1800 136 066
Email: hsc@dhs.vic.gov.au

- Western Australia
  The Office of the Information Commissioner
  Tel: 1800 621 244
  Email: info@foi.wa.gov.au

Privacy issues

There are a number of broad privacy-related issues that face general practitioners and other primary health care providers. These include:

- Collecting information

Normally, general practitioners should only collect health information about patients with their consent. It is usually reasonable to assume that consent is implied if the information is noted from details provided by the patient during a consultation, as long as it is clear that the patient understands what information is being recorded and why. It is also vital to ensure that record keeping is thorough and accurate: both to ensure the best-possible ongoing treatment of a patient and, in the worst-case scenario, to be used as defence if a case is made against a treating doctor.

- Ensuring consent is 'informed'

All medical procedures require informed consent. Given that the consequences of being tested may be substantial, it is important to realise that, while running tests may be standard for the health care practitioner, receiving the results may be anything but routine for the patient. The provision of information should allow the health care practitioner to discuss the risks and benefits to the patient in their particular situation, thereby facilitating their decision-making process.

- Advising use

Patients are not able to consent to the use of their information if they are unclear where the information will go and why. If possible, patients should be advised of the use of their information when it is collected, which can occur through usual communication during a regular consultation. This point also relates to instances when personal information cannot be shared or disclosed. In a recent legal case, a doctor failed to inform two patients attending a joint consultation that the results of each person's test could not be disclosed to the other person, and consequently failed to seek either their understanding of that situation or their consent for their test results to be shared. Please refer to ASHM Viral Hepatitis Models of Care Models of Care database for a summary of relevant case law (available at www.ashm.org.au/hvb-moc/).

- Notification

It might be argued that reporting details of a patient's health status involves breaching his or her privacy, however, this practice is legal because there is no 'absolute' right to privacy under Australian or international law. The Privacy Act provides exceptions to privacy where use or disclosure is required by law. In developing Australian privacy laws, the right to individual privacy has been weighed against the rights of others and against matters that benefit society as a whole.

HBV is a notifiable disease in all Australian States and Territories. Legal obligations around notification are mandated by State laws, which define a doctor's duty to notify the respective Health Department of a notifiable disease. In NSW, for example, the Public Health Act 1991 requires doctors to notify their local Public Health Unit by phone or mail of any cases of acute viral hepatitis. Notifications are not to be made by facsimile, in order to protect patient confidentiality. Doctor and hospital notification forms are available at http://www.health.nsw.gov.au/public-health/forms.

- Accessing personal records

Patients are entitled to access their health records, except for a limited number of important exceptions outlined under NPP 6, for example if the request for access is frivolous or vexatious, or providing access would be likely to prejudice an investigation of possible unlawful activity. The full list of NPP 6 exceptions are listed at http://www.privacy.gov.au/publications/npps01.html#npp6. The Office of the Privacy Commissioner's fact sheet relating to access is available at http://www.privacy.gov.au/publications/IS4_01.html.

Patients, including an index case (original person identified with an infection) or a contact, are not entitled to any information that relates to their contact's identity, behaviour or diagnosis without that person's consent, even if that information is in the patient's records. Should a patient wish to access their own record, details of the identity of any contacts contained in their record should be deleted.

- Security and storage of health information

A range of laws apply to the storage of health information. Health agencies should have in place:

- Procedures to give access to information only to those people who are authorised to have access in order to use or disclose the information
- Security measures to prevent unauthorised access to the records
- Procedures for storing the information, where practical, in a way that the identity of the person is not readily apparent from the face of the record, e.g. by the use of identification codes
- Procedures for destroying the records that protect the privacy of the information.

Electronic records pose new challenges. While they offer greater convenience of data retrieval and transfer, electronic record systems also create greater risks of data leakage, access by unauthorised staff and 'browsing' by unauthorised people. Agencies and businesses, including medical practices need to consider the security of their data storage and transfer systems and the problem of staff intentionally multidisciplinary team how this will affect the handling of their health information. It is also advisable to gain patient consent to avoid relying on implied consent. Other limited exceptions under NPP 2 permit disclosure without consent in certain circumstances, including to lessen a serious and imminent threat to an individual's life, health or safety; or where the disclosure is required or authorised by law.

There is a need for doctors in group practices to formulate clear internal communication protocols in order to exercise reasonable care, for example, when communicating test results or considering contact tracing issues. The cross-referencing of files per se will generally not breach statutory confidentiality because results need to be checked, though information should not be disclosed without explicit permission. It is vital that all staff are aware of their obligations and that systems are in place for protecting patient privacy.

Exemptions to privacy and confidentiality obligations

The use and disclosure of health information is defined in the Privacy Act under NPP 2

or inadvertently accessing prohibited electronic records. This issue is currently being addressed by the Commonwealth and a number of States in the development of their electronic health records systems, and has proven enormously complex to date.

- Information for teams

Multidisciplinary treating teams are common practice in Australian health care. Health care practitioners work together and share necessary information to deliver optimum health care. All transfers of information without the knowledge of the patient require careful ethical consideration.

Although the question has not yet been legally tested, private sector health service providers do not always require a patient's consent to disclose specific health information to another member of a multidisciplinary team for a health care purpose, as long as the patient would reasonably expect that disclosure. Therefore, it is advisable to tell a patient being treated by a

- not possible to conceal the identity of the source patient who has refused to consent to disclosure
- Provision of medical services in a particular instance of care where there is a need to know the patient's infection status for treatment purposes of benefit to the patient (e.g. in an emergency or if the patient is unconscious). This should not, however, detract from the observance of standard infection control precautions.

It is strongly recommended that practitioners familiarise themselves with the National Privacy Principles (which are legally binding) and contact the Office of the Privacy Commissioner if they wish to clarify the manner in which

the National Privacy Principles might relate to specific situations. Legal advice should be sought from a legal practitioner.

Contact tracing

The practice of contact tracing raises the

question of potential conflict between breaching a patient's privacy and confidentiality, and alerting a third party to the fact that they may be at risk of HBV infection. Although a case on this specific point is yet to be heard in Australia, it seems likely that a health practitioner could be found negligent to a third party if they did not warn the third party that they were at risk. This potential conflict may be further complicated by a statutory obligation to counsel patients regarding sexually transmissible medical conditions.

Fortunately, public health services afford practitioners expert guidance to resolve the conflict between the duties to maintain confidentiality and privacy, and a possible duty of care owed to third parties. In instances where practitioners suspect a person may

be putting others at risk, the practitioner

should notify the health department using the methods prescribed by the relevant State or Territory. Public health authorities then become responsible for making decisions around contact tracing, including the management of privacy issues. For a more detailed account of the contact tracing responsibilities of health care providers, please consult the Australasian Contact Tracing Manual Ed 3, available at: http://www.ashm.org.au/contact-tracing/ .

(available at http://www.privacy.gov.au/publications/npps01.html#npp2), which states that an organisation must not use or disclose personal information about an individual for a purpose other than the primary purpose of collection, except for a number of situations, including where an organisation reasonably

- believes that the use or disclosure is necessary to lessen or prevent a serious and imminent threat to a person's life, health or safety, or a serious threat to public health or public safety.

In short, health care workers must not disclose a person's health information except in a very limited number of circumstances. These may generally be summarised as:

- Communicating necessary information to others directly involved in the treatment of a patient during a particular episode of care
- Cases of needlestick injury where a professional is aware of a patient's HBV positive status, and a health care worker has been exposed to circumstances where there is a real risk of transmission and it is

Criminal law

There are two types of criminal offences associated with HBV and other blood-borne

- viruses. The first relates to the disclosure of information regarding a person who has an infection, or is suspected of having HBV or other blood-borne virus infections—as discussed above. There are also laws in every State and Territory making it an offence to transmit an infection to another person. As with other areas of legislation, specifications around definition and scope differ across jurisdictions. The majority of these laws are not specific to blood-borne viruses, but instead refer to infectious diseases generally; more generic criminal offences, for example, causing grievous bodily

harm, may also be applied.

Anti-discrimination

Anti-discrimination provisions exist across all Australian States and Territories, making it illegal to discriminate against people on

the basis of their (perceived) HBV infection.

Discrimination is prohibited on the basis of disability or impairment. It is important that health care practitioners consider behaviours they must avoid when testing and managing people with HBV. Discrimination on the basis of disability or impairment includes treating a person less favourably as a result of their (perceived) disability or impairment. In a health care setting, this may include refusing to see a patient, offering different or inappropriate treatment, or placing a patient last on a consultation or operating list. As outlined in Chapter 11: Infection control and occupational health, standard precautions ensure a high level of protection against the transmission of infection in the health care setting and represent the level of infection

control required in the treatment and care of

all patients to prevent transmission of blood-

borne infections.

Health care workers with HBV infection

Please refer to Chapter 11: Infection control and occupational health for obligations of health care practitioners who perform exposure prone procedures.

Australian Privacy Laws and Health Information

http://www.statecapitalgroup.org/meetings/san%20francisco/Australian%20Privacy%20Law%20Reform%20and%20Health%20Information%20Articles%20October%202013.pdf
December 08, 2014

Collection – research etc. A "permitted health situation" exists in relation to the collection by an organisation of health information about

Australian Privacy Laws and Health Information
Author: Alison Choy Flannigan, Partner, Holman Webb Lawyers, Sydney Australia
October 2013

Australia privacy rights are regulated by Commonwealth and State legislation and the laws protecting confidential information under the common law.

Australian privacy laws govern the collection, use and disclosure of “personal information”. Further, individuals are provided with a right of access and correction of their own personal information. There are also data security, data quality and cross-border transborder data flow requirements.

Under Australian privacy laws:

- “personal information” means information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion”

In Australia, health information (such as medical records) are a subset of personal information and attract additional protection and rules. These include:

- Use and disclosure is permitted if there is a serious and imminent threat to the health and safety of an individual or the public;
- Use and disclosure for health and medical research if certain conditions are met;
- Disclosures to carers for compassionate reasons;
- Restrictions on access if providing direct access would pose a serious threat to the life or health of any individual
- Use and disclosure of genetic information to lessen or prevent a serious threat to a genetic relative.

“health information” means:

(a) information or an opinion about:

(i) the health or a disability (at any time) of an individual; or

(ii) an individual’s expressed wishes about the future provision of health services to him or her; or

(iii) a health service provided, or to be provided, to an individual; that is also personal information; or

(b) other personal information collected to provide, or in providing, a health service; or

(c) other personal information about an individual collected in connection with the donation, or intended donation, by the individual of his or her body parts, organs or body substances; or

(d) genetic information about an individual in a form that is, or could be, predictive of the health of the individual or a genetic relative of the individual.

- “health service” means:

(a) an activity performed in relation to an individual that is intended or claimed (expressly or otherwise) by the individual or the person performing it:

(i) to assess, record, maintain or improve the individual’s health; or

(ii) to diagnose the individual’s illness or disability; or

(iii) to treat the individual’s illness or disability or suspected illness or disability; or

(b) the dispensing on prescription of a drug or medicinal preparation by a pharmacist.

The Privacy Act 1988 (Commonwealth) (Privacy Act), which applies to Australian Commonwealth government agencies and private sector organisations, has been recently amended by the Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth) (Privacy Amendment Act). The Privacy Amendment Act was passed by Parliament on 29 November 2012, received the Royal Assent on 12 December 2012 and comes into force on 12 March 2014.

The amendments aim to:

- create a single set of Australian Privacy Principles applying to both Australian Government agencies and the private sector. These principles will replace the existing Information Privacy Principles and National Privacy Principles;
- introduce more comprehensive credit reporting, improved privacy protections and more logical, consistent and simple language;
- strengthen the functions and powers of the Australian Information Commissioner to resolve complaints, use external dispute resolution services, conduct investigations and promote compliance- penalties of up to 2000 penalty units $340K for individuals – x 5 for body corporates AUD$1.7 million; and
- create new provisions on privacy codes and the credit reporting code, including codes that will be binding on specified agencies and organisations.

Australian Privacy Principles
The Privacy Amendment Act introduces a unified set of Australian Privacy Principles which apply to both Commonwealth agencies and the Australian private sector, replacing separate public and private sector principles.

Permitted health situations
The Privacy Amendment Act introduces the concept of “permitted health situation” in a new section 16B.

Collection – provision of a health service
A “permitted health situation” exists in relation to the collection by an organization of health information about an individual if:

(a) the information is necessary to provide a health service to the individual; and
(b) either:

(i) the collection is required or authorised by or under an Australian law (other than the Privacy Act); or
(ii) the information is collected in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation.

Collection – research etc.
A “permitted health situation” exists in relation to the collection by an organisation of health information about an individual if:

(a) the collection is necessary for any of the following purposes:
(i) research relevant to public health or public safety;
(ii) the compilation or analysis of statistics relevant to public health or public safety;
(iii) the management, funding or monitoring of a health service; and
(b) that purpose cannot be served by the collection of information about the individual that is de-identified information; and
(c) it is impracticable for the organisation to obtain the individual's consent to the collection; and
(d) any of the following apply:
(i) the collection is required by or under an Australian law (other than the Privacy Act);
(ii) the information is collected in accordance with rules established by competent health or medical bodies that deal with obligations
of professional confidentiality which bind the organisation;
(iii) the information is collected in accordance with guidelines approved under section 95A of the purposes of this subparagraph.

Use or disclosure – research, etc.
A "permitted health situation" exists in relation to the use or disclosure by an organisation of health information about an individual if:
(a) the use or disclosure is necessary for research, or the compilation or analysis of statistics, relevant to public health or public safety; and

(b) it is impracticable for the organisation to obtain the individual's consent to the use or disclosure; and
(c) the use or disclosure is conducted in accordance with guidelines approved under section 95A for the purposes this paragraph; and
(d) in the case of disclosure – the organisation reasonably believes that the recipient of the information will not disclose the information, or personal information derived from that information.

Use of disclosure – genetic information
A "permitted health situation" exists in relation to the use or disclosure by an organisation of genetic information about an individual (the first individual) if:
(a) the organisation has obtained the information in the course of providing a health service to the first individual; and
(b) the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of another individual who is a genetic relative of the first individual; and
(c) the use or disclosure is conducted in accordance with guidelines approved under section 95AA; and
(d) in the case of disclosure – the recipient of the information is a genetic relative of the first individual.

Disclosure – responsible person for an individual
A "permitted health situation" exists in relation to the disclosure by an organisation of health information about an individual if:
(a) the organisation provides a health service to the individual; and
(b) the recipient of the information is a responsible person for the individual; and
(c) the individual:
(i) is physically or legally incapable of giving consent to the disclosure; or
(ii) physically cannot communicate consent to the disclosure; and
(d) another individual (the carer) providing the health service for the organisation is satisfied that either:
(i) the disclosure is necessary to provide appropriate care or treatment to the individual; or
(ii) the disclosure is made for compassionate reasons; and
(e) the disclosure is not contrary to any wish:
(i) expressed by the individual before the individual became unable to give or communicate consent; and
(ii) of which the care is aware, or of which the carer could reasonably be expected to be aware; and
(f) the disclosure is limited to the extent reasonable and necessary for a purpose mentioned in paragraph (d).

Please contact Alison Choy Flannigan with any questions.

Alison Choy Flannigan, Partner, Holman Webb
P: +61 2 9390 8338
E: alison.choyflannigan@holmanwebb.com.au

This article is provided for general information purposes only and should not be relied upon as legal advice.

Update on Personally Controlled Electronic Health Records - Legal and Privacy Issues

Alison Choy Flannigan, Partner, Holman Webb Lawyers, Sydney Australia

October 2013

As part of the 2010/11 Federal budget, the Government announced a $466.7 million investment over two years for a national Personally Controlled Electronic Health Record (PCEHR) system for all Australians who choose to register on-line, from 2012-2013. This initiative has the potential to be a revolutionary step for Australian health care, in terms of both consumer's access to their own health information and improvement in information which will be available to health professionals when they treat a patient.

To date, the uptake has been slow. NeHTA scorecard as at July 2013

- The total number of people who registered for an eHealth record as at May 31 2013 was 612,391.
- More than 4,502 healthcare provider organisations have signed onto the eHealth Record system.
- 6567 individual doctors, nurses and other healthcare providers throughout Australia has been authorized by their organisations to access the PCEHR system;
- More than 15.25 million documents have been uploaded into the PCEHR system.

Aims of PCEHR include:

- Reduce risks in the health system;
- Fewer patients will experience adverse events
- Improve access to health records and thereby reduce medication errors.

Some key concepts are:

• Individuals are able to choose whether or not to have a PCEHR and will be able to set their own access controls and may withdraw at any time.
• The PCEHR will contain clinical documents such as Shared Health Summaries, Discharge Summaries, Event Summaries, Pathology Result Reports, Imaging Reports and Specialist Letters. It may also include key health information entered by the individual such as over-the-counter medicines and allergies and access information

5

from Medicare Australia such as an individual's organ donor status, dispensed medications funded under the PBS, information about healthcare events from an individual's Medicare claiming history and a child's immunisation history. The PCEHR may also contain an individual's advance care directives (if any). The PCEHR is, however, not a comprehensive health record.
• Healthcare organisations can choose to participate and will need a healthcare organisation identifier (HPI-O). They must agree to use appropriate authentication mechanisms to access the PCEHR and use software that has been conformance tested to be used with the PCEHR system.
• Health information within the PCEHR system is protected through a combination of legislation, governance arrangements and security and technology measures, including under the Personally Controlled Electronic Health Records Act 2012 (Cth).

The PCEHR legislation imposes penalties for intentional or reckless unauthorized collection, use and disclosure of health information; Fines up to 120 penalty units for individuals (AUD$20,400); and x 5 penalties for bodies corporate AUD$102,000. One Commonwealth penalty unit is currently AUD$170.

There are a number of medico-legal and privacy issues which arise with the PCEHR. Some of these are summarised below:

Medico-legal
• If a medical practitioner consults with a patient and is negligent in entering information onto the PCEHR, there are more clinicians relying upon it, so the potential for liability from a negligent assessment of a patient or negligently prepared medical record increases.
• Health professionals must be mindful that the PCEHR is not a complete medical record and must continue to be vigilant in continuing to obtain independent information from patients. Information may be excluded from the PCEHR at the request of a patient and missing information is unlikely to be flagged.
• If a medical practitioner has relied upon information on the PCEHR which is incorrect, then the medical practitioner will need to track the author of the original information to join as a cross-defendant.
• If a patient instructs a medical practitioner not to include information on the PCEHR then the medical practitioner will be under an obligation to inform the patient the risks and consequences of this.
• Direct access to a medical record may be denied if providing access would pose a serious threat to the life or health of any individual. In those cases, the patient is usually provided access through another medical practitioner. If consumer access requests are dealt with centrally, measures should be implemented to ensure that a clinical assessment is made in relation to whether or not a patient's request for access or information could pose a serious threat to the life or health of any individual. Arguably such information should not be included in the PCEHR.
• Often a request for access can be an indicator of a potential claim which can be resolved quickly by the clinician by early discussions with the patients. There should be a mechanism so that relevant clinicians are informed if there is a potential claim early.

Privacy issues
There are also a number of privacy issues, including:

6

• Obtaining adequate privacy consent from patients;
• Ensuring that the systems can accurately implement the consent options of patients, such as limiting access or prohibiting access to the PCEHR to health professionals nominated by patients.
• Ensuring that only information which is required to provide treatment for the patient is collected.
• Privacy issues if the system involves a number of system vendors and subcontractors or cloud computing.
• Uniformity of the usage of medical terms and abbreviations and clear handwriting is preferred to protect data quality.
• Clear understanding of the information flows and potential for leakage of personal health information to unapproved persons or overseas.
• Data security issues.
• Patient and participating health professional identification and verification issues.
• Education and training of participating health professionals.

Please contact Alison Choy Flannigan with any questions.

Alison Choy Flannigan
Partner, Holman Webb
T: +61 2 9390 8338
E: alison.choyflannigan@holmanwebb.com.au

7

Mobile Medical Apps – When are they medical devices?

Alison Choy Flannigan, Partner, Holman Webb Lawyers, Sydney Australia

October 2013

Like the US, Australia is experiencing the proliferation of mobile medical apps (software applications that can be executed on a mobile platform) which seek to provide a number of functionalities, many of which operate between traditional disease management and health and wellness. Some of these new apps assist consumers with their health and wellness management, whilst others provide healthcare providers with tools to improve and facilitate the delivery of patient care.

United States

The US Food and Drug Administration (FDA) released the Mobile Medical Applications Guidance for Industry and Food and Drug Administration Staff on 25 September 25 2013.

The US Guidance explains how the FDA intends to regulate select software applications intended for use on mobile platforms.

The FDA defines a “mobile medical app” as a mobile app that meets the definition of “device” in section

201(h) of the Federal Food, Drug, and Cosmetic Act (FD&C Act) and includes an application that:

• is used as an accessory to regulated medical device, for example a remote display to a medical monitor; or

• transforms a mobile platform into a regulated medical device, for example an attachment to a blood glucose strip.

The intended use of the mobile app determines whether it meets the definition of a “device”. As stated in 21 CPR 801.4, intended use may be shown by labelling, claims, advertising materials, or oral or written statements by manufacturers or their representatives. When the intended use of a mobile app is for the diagnosis of disease or other conditions, or the cure, mitigation, treatment, or prevention of disease, or is intended to affect the structure or any function of the body of man, the mobile app is a device.

The FDA intends to apply its regulatory oversight to only those mobile apps that are medical devices and whose functionality could pose a risk to a patient’s safety if the mobile app were not to function as intended.

Mobile medical apps that meet the definition of a device must follow the regulation required for the particular class of device classification.

8

The FDA will apply regulatory oversight in respect of applications which allow the user to input patient-specific information and, using patient-specific formulae or algorithms, output a patient-specific result, diagnosis or treatment recommendation to be used in clinical practice or to aid in making clinical decisions.

There are three categories:

1. Mobile apps which are not medical devices;
2. Mobile medical apps which may be medical devices and for which the FDA intends to exercise enforcement discretion (meaning that the DFA does not intend to enforce requirements under the FD& C Act; and
3. Mobile medical apps which are the focus of FDA’s regulatory oversight (mobile medical apps);

The US Guidance does not consider the following as medical apps:

- mobile apps containing only medical reference materials or educational tools for medical training, which do not contain patient specific information;
- mobile apps that are intended for general patient education and facilitate patient access to commonly used reference information, treatment, or prevention of a disease;
- mobile apps that automate general office operations in a healthcare setting and are not intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation;
- medical apps which are generic aids, for example a magnifying glass; and
- mobile apps that perform the functionality of an electronic health record system.

Examples of mobile apps which may meet the definition of medical devices but which the FDA intends to exercise enforcement discretion because they pose lower risk to the public include:

- mobile apps that help patients with diagnosed psychiatric conditions by providing a “skill of the day” behavioral technique or messages which can be accessed to decrease anxiety;
- mobile apps that us GPS location information to alert asthmatics of environmental conditions;
- mobile apps which use video and video games to motive patients to do their physical therapy exercises at home; and
- mobile apps which advise on interactions between herbs and drugs.

The following are examples of regulated mobile apps:

- mobile apps that transform a mobile platform into a regulated medical device, such as mobile apps which use a sensor or electrode to measure blood oxygen saturation;
- mobile apps that connect to an existing device type for the purposes of controlling its operation, function or energy source, for example, a mobile app which controls an infusion pump or a cochlear implant;
- mobile apps that display, transfer, store or convert patient-specific medical device data from a connected device, for example, a device which connects to a nursing central station and displays medical data to a physician’s mobile phone.

Manufacturers of mobile medical devices are subject to the requirements described in the applicable device classification regulations.

9

Australia

The Australian Therapeutic Goods Administration (TGA) regulates the quality, safety and performance of medical devices and uses a regulatory framework that includes software for therapeutic purposes which falls under the definition of a “therapeutic good” under the Therapeutic Goods Act 1989 (Cth)(Act).

In Australia, whether or not a mobile health and medical app is a “medical device” and “therapeutic good” (and regulated as such) depends principally upon:

1. functionality; and

2. the claims made in relation to the product

Therapeutic goods includes goods that are represented in any way to be, or that are, whether because of the way in which the goods are presented or for any other reason, likely to be taken to be for “therapeutic use” (as defined) and includes medical devices, subject to stated exceptions.

Section 41BD of the Act states that

A medical device includes:
(a) any instrument, apparatus, appliance, material or other article (whether used alone or in combination, and including the software necessary for its proper application) intended, by the person under whose name it is or is to be supplied, to be used for human beings for the purpose of one or more of the following:

i. diagnosis, prevention, monitoring, treatment or alleviation of disease;

ii. diagnosis, monitoring, treatment, alleviation of or compensation for an injury or disability;

iii. investigation, replacement or modification of the anatomy or of a physiological process;

iv. control of conception; and that does not achieve its principal intended action in or on the human body by pharmacological, immunological or metabolic means, but that may be assisted in its function by such means; or
b. an accessory to an instrument, apparatus, appliance, material or other article covered

by paragraph (a).

The Medical Technology Association of Australia (MTAA) in its submission on Apps Purchases by Australian Consumers on Mobile and Handheld Devices dated January 2013 recommended the "regulation of smartphone medical apps that are intended by the developer to cure, treat, monitor or diagnose a medical condition."

10

In that paper the MTAA mentions that the TGA has stated that it will regulate health apps for smartphones as the need arises.

Please contact Alison Choy Flannigan with any questions.

Alison Choy Flannigan, Partner

Holman Webb, Lawyers

Health, aged care & life sciences

E:alison.choyflannigan@holmanwebb.com.au

P: +61 2 9390 8338

11

Internet privacy: how Australia's new laws will work

http://www.theguardian.com/world/2014/feb/04/internet-privacy-how-new-laws-work December 08, 2014

Internet privacy: how Australia's new laws will ... New privacy laws will come into operation in ... steps to ensure data is used in accordance with Australia's laws.

New privacy laws will come into operation in Australia in March this year. The amendments to the Privacy Act will introduce a new and harmonised set of privacy principles. While there is still plenty of room for improvement, the new laws make some important steps in protecting privacy, particularly with the collection of data online.

The new reforms apply to all bodies that collect or store personal information about Australians. They don't operate in a vacuum; there is a broad (if somewhat patchwork) frame of privacy laws across the globe, and the way that they interact with some of these different laws will be interesting to follow in coming years. Here's a guide to some of the changes and some comments from Australia's information commissioner, Professor John McMillan, on the changes.

Organisations that collect personal data must take reasonable steps to notify an individual user about that collection. They need to tell you about the circumstances of collection and its purpose. So when you visit a website they need to tell you if they are collecting information on your browsing habits, and the purpose of that collection.

There is a loophole in this principle that could give some wiggle room on this – the act also allows organisations to provide notification of data collection after it has actually been collected, "as soon as possible after".

The information commissioner said his office would be ensuring there was oversight of those kind of retrospective collections: "The term 'reasonable steps' is an objective standard, and what it requires any entity to do is to point to why it gave notification and to explain why that was a reasonable step and point to evidence that backs up what it's doing."

One of the most significant changes is stronger laws governing the sending of data overseas. Australians' data is routinely sent overseas, and the new principles attempt to impose a greater burden to the entity that sends the data overseas, by stating the entity in Australia must take "reasonable steps" to ensure the principles are not breached overseas.

McMillan says a good example of reasonable steps could be contractual measures. So if a cloud service provider is planning on sending data overseas, it should have a contract in place to make sure data will not be misused.

Once again there is an exception that some organisations may attempt to rely on. If the overseas entity is subject to a "substantially similar" privacy law it does not have to take reasonable steps to ensure data is used in accordance with Australia's laws. The question of what is a substantially similar regime is not clear, and McMillan said his office would not be compiling a global list of accredited regimes; each would be decided on a case by case basis.

"It's not practical for us as a little office to do a global analysis and draw up an accredited list. Privacy regulators elsewhere have faced the same thing and they shy away from the difficulty of drawing up that list. The message you get from that is the onus is on the individual entity to ensure adequate privacy protection."

The reforms also create a stronger right to access personal information from private entities. While it was already possible to access personal information from government agencies under freedom of information laws, the privacy reforms take this a step further – there is now a separate right to request information from private corporations and entities that could hold personal information.

An obvious example of this is for companies such as Facebook and Google – in theory you can now find out how much data they hold on you, what format they hold it in, and whether they have disclosed that information to other parties. The entities are obliged to provide the information to you, but can impose some charges if there is a cost to retrieving the information.

The right of access is more flexible than under the Freedom of Information Act. Private organisations only need to respond in a "reasonable amount of time" but the commissioner's guidelines suggest that 30 days would be reasonable in most situations. You also cannot appeal against an adverse decision to the commissioner's office – but you can still lodge a complaint with the commissioner, which might be able to assist in getting hold of the information.

The information commissioner's powers have been strengthened under the reforms, allowing him to impose tougher penalties and issues binding decisions resulting from investigations and review applications. The limited resources provided to the commissioner may be an issue in enforcing

this, particularly if the commissioner needs to go to the federal court to impose penalties on an entity; the court costs would have to be borne by the commissioner, a cost his office currently cannot afford under its budget.

Australian organisations unprepared for new privacy laws: McAfee

http://www.zdnet.com/au/australian-organisations-unprepared-for-new-privacy-laws-mcafee-7000014636/ December 08, 2014

As the Australian Privacy Commissioner and Attorney-general warn businesses to prepare themselves for upchanges to the Privacy Act, McAfee has found that ...

Summary:As the Australian Privacy Commissioner and Attorney-general warn businesses to prepare themselves for upchanges to the Privacy Act, McAfee has found that most don't even realise that there are changes or fines for non-compliance.

A survey of business and government agencies has found that many are largely unaware of upcoming changes to the Australian Privacy Act under which large fines may be imposed if consumer data is not adequately protected.

The April survey, commissioned by internet security company McAfee, found that 59 percent of employees responsible for managing the personal information of customers were unaware or unsure of the changes.

From March 2014, organisations subject to the amended Privacy Act could face penalties ranging from $340,000 for individuals and $1.7 million for corporations. These fines are the maximum civil penalties that the Privacy Commissioner will be able to hand down to organisations for serious or repeated violations of the Australian Privacy Principles they are bound by.

Earlier on Monday, the Privacy Commissioner and the Attorney-general warned businesses that they need to start preparing for the changes now.

The research also showed that more than one in five organisations admitted to data breaches, and nearly half of the employees managing customer's personal information hadn't received training in managing and storing sensitive data.

Of those that were aware of the upcoming changes to the Privacy Act, just under half had taken action in the form of conducting a privacy impact assessment. Of the action-takers, 46 percent also reviewed their existing technology controls, and 33 percent sought legal advice.

Meanwhile, in terms of the data being collected by organisations, some believe that businesses are overstepping their bounds when it comes to asking customers for information.

Honorary Associate Professor Terry Beed from the University of Sydney Business School said that consumer information is being amassed in a way that does not comply with the code governing data collection by market and social researchers.

He said that market research tools such as SurveyMonkey are now readily available to individuals or firms who may not use them correctly or ethically.

"The ground is changing under our feet," he said in a statement on Monday.

"There has been an explosion in the amount of personal data being gathered in the digital environment, and it has revolutionised the way we go about marketing goods and services."

Beed said that much of the data was being gathered by people with no background in market and social research.

He said that it's important they are educated about working with consumers' personal information in accordance with the privacy regulations.

Much of the data is being on-sold to marketers, often via data brokers, without the knowledge or consent of consumers, and in possible breach of the privacy codes approved by the Australian Privacy Commissioner.

Beed said the use of age, gender, or product preferences to design highly targeted advertising may be annoying to some consumers, but is relatively harmless.

"Of far greater concern is data that might be related to incomes, debt levels, or health profiles, which is gathered and on-sold without any warning to the consumer."

His viewpoints are matched by Stephen Wilson, managing director of digital identity company Lockstep Consulting. Wilson highlighted at the Sydney launch of Privacy Awareness Week on Monday that technologists often don't understand their obligations under the Privacy Act, or even that the information they are collecting is considered personal information.

"Personal information is thought to be the stuff of forms, questionnaires, call centres, and the like. Technologists can be really surprised when they find that the definition encompasses things like metadata, event logs, and the stuff of technology that's personally identifiable," Wilson said.

He drew a parallel to the Google Streetview case, where Google was found to be in breach of the Australian Privacy Act to the surprise of many technologists that felt that if a wireless hotspot were broadcasting information in to the public domain, it should not be considered private.

"If the data is in the public domain, the technologists held that it was up for grabs, and that Google cannot have done anything wrong," Wilson said.

"[But] it doesn't matter where you got the information from. You can get information from the public domain and you've still committed a collection [of personal information]."

He also highlighted that many of the leading edge insights into big data often overshadowed the need to respect Australia's privacy principles. He ran through a brief example of a paper published in Science that found that despite certain donated genetic data (such as the 1,000 Genomes Project) being made anonymous, researchers had been able to match the information to genealogy databases, and thus narrow down individuals based on demographic information and other public records.

While noting how remarkable the research was, he said that it could also be considered in violation on Australia's current National Privacy Principles.

"If you put a name on something that was previously anonymous, you've collected data, and you probably need to get the consent of the person because it's a third party and they've got no prior relationship."

Privacy Law in Australia: an overview - Gilbert + Tobin ...

http://www.gtlaw.com.au/wp-content/uploads/Privacy-Law-in-Australia-an-overview.pdf December 08, 2014

Practical remedies for Australians adversely affected by privacy invasive practices of businesses may also be available through the operation of binding APP codes and ...

Privacy Law in Australia: an overview
Peter Leonard, Gilbert + Tobin Lawyers and iappANZ Director

March 2014

1 A quick guide to the changes

The Privacy Act 1988 (Privacy Act) was amended by the Privacy Amendment (Enhancing Privacy Protection) Bill 2012. The amendments took effect on 12 March 2014.

The amendments generally add provisions and corresponding compliance obligations.

Two Parts of the Privacy Act are completely replaced.

Part IIIA of the Privacy Act, dealing with credit reporting, is replaced in full by new credit information provisions. There are important changes to the current framework as to credit information policies, the collection and recording of credit related information, and disclosure of credit related information to overseas entities. Banks, retail businesses that issue credit cards, entities who carry on businesses which substantially involve the provision of credit, suppliers of goods and services on credit/payment terms, equipment lessors and hire purchase credit providers are 'credit providers' and must comply with the new framework. That framework is then expanded through a revised Credit Reporting Privacy Code prepared by the Australian Retail Credit Association and registered by the Australian Privacy Commissioner (Commissioner) in January 2014 following a lengthy consultation period. The Code also took effect on 12 March 2014. The Code is available at http://www.oaic.gov.au/privacy/applying-privacy-law/privacy-registers/credit-reporting-privacy-code.

The National Privacy Principles (NPPs) (for private entities, but subject to the small business exception) and Information Privacy Principles (IPPs) (for government entities) are replaced with a single regime of privacy principles, the Australian Privacy Principles (APPs). The APPs are available at (http://www.oaic.gov.au/privacy/privacy-resources/privacy-fact-sheets/other/privacy-fact-sheet-17-australian-privacy-principles. The APPs generally apply to Federal and ACT government agencies and organisations alike; however, some APPs draw distinctions in the coverage of government agencies and private sector entities.

Probably the key change is through APP 1 (privacy policy) and APP 5 (notification obligations), which place a higher onus on entities to institute practices, procedures and policies in relation to the protection of privacy. Many entities continue to focus upon policies and general disclosures and place insufficient emphasis upon the development of processes and procedures that ensure that the policies are in fact implemented and this implementation is effective, reliable and verifiable. Such entities will find the developing focus of the Privacy Commissioner upon whether an entity has taken all reasonable and practical steps to implement policies, rather than just write and publish policies, as a novel compliance challenge.

Among other implementation challenges, an entity must ensure:

- that it can demonstrate that user consent had been obtained (when consent is in issue), and
- that the entity has in place effective procedures to deal with inquiries and complaints about an entity's compliance with the APPs and any applicable registered APP code of practice (when such codes are registered and apply to such organisations).

That is not to suggest that stated privacy policies and collection notices have become less important: to the contrary, the Act has become more prescriptive as to their form, substance, accessibility and intelligibility. A privacy policy must be 'transparent', accessible to the public and available free of charge. A privacy policy will need to include details as to:

- specific kinds of personal information that the entity collects and holds and how it is collected and held;
- purposes (both primary and secondary) for which the entity collects, holds, uses and discloses personal information;
- how an individual may access personal information about the individual that is held by the entity and seek the correction of such information;
- how an individual may complain about a breach of the APPs or an applicable registered APP code; and
- how the entity will deal with a complaint (entities will also need to ensure that internal procedures are implemented consistently with this description, including by appropriate training of staff).

Other changes include:

- APP 2 (anonymity and pseudonyms), which provides that where practicable individuals must not be required to disclose their identity and may use a pseudonym. Previously there was only the requirement to provide an option of anonymity: the requirement to allow the use of pseudonyms (where practicable) is new;
- APP 4 (unsolicited personal information), which provides that where an entity receives unsolicited personal information that it could not have obtained through solicited means on reasonable terms, the entity must destroy the information;
- APP 5 (notification of collecting personal information), which is much more prescriptive than the former provision dealing with this subject matter, NPP 1. At or before the time information is collected, or if that is not practicable, as soon as practicable after information is collected, the collecting entity must ensure that it informs an affected individual of certain matters, including that the information has been collected; the purpose of collection; the consequences for the individual if the information is not collected; the procedure to complain about or amend information and any third parties that the information may be disclosed to; and
- APP 7 (direct marketing), which increases requirements for informed user consent in relation to direct marketing. Entities must have a simple means by which an individual can readily request not to receive direct marketing from the entity and ensure that personal information about the individual is not provided to third parties for the purpose of direct marketing.

Probably the most controversial and least understood change is new section 16C and APP 8 (disclosure to overseas entities).

APP 8 introduces a new 'accountability principle' to the effect that where an Australian entity intends to

disclose (including disclosure through provision of electronic viewing access – a physical data transfer is not required) personal information to an overseas entity, the Australian entity must 'take such steps as are reasonable in the circumstances to ensure' that the overseas entity complies with the APPs in respect to the provided information. If the overseas entity does not comply with the APPs in respect to the provided information, then the Australian entity is 'accountable' and liable pursuant to section 16C

as if it had not complied itself. This is the case regardless of whether the Australian entity had in fact taken reasonable steps to ensure that the overseas entity complied with the Privacy Act, or failed to take such steps. Accordingly, entities considering providing personal information to overseas entities will need to consider contractually binding such overseas entities to comply with the new privacy legislation and the Australian entity's privacy policy, including as to implementation of privacy safeguards, and the legal exposure of the Australian entity if the overseas entity fails to comply with that contract and implement and observe those safeguards. There are a number of important exceptions to this 'accountability' rule: these exceptions are discussed in section 20 (Cross-border disclosure) of this paper.

From March 2014, the Commissioner's investigative and enforcement powers are significantly enhanced. Powers will include a right for the Commissioner to seek a Court injunction against a person engaging in conduct that may contravene the Privacy Act, to obtain enforceable undertakings by a person that has breached the Privacy Act, and to seek the making by a Federal Court of civil penalty orders where there is either a serious or repeated interference with the privacy of an individual.

These and other changes taking effect from March 2014 or otherwise mooted are examined in more detail in later sections of this paper.

On 21 February 2014 the Commissioner released the Australian Privacy Principles (APP) Guidelines (available at http://www.oaic.gov.au/privacy/applying-privacy-law/app-guidelines/). As stated by the Commissioner, "The APP guidelines outline the mandatory requirements of the APPs, how the OAIC will interpret the APPs, and matters we may take into account when exercising functions and powers under the Privacy Act". These Guidelines are therefore of significant interest as an expression of the Commissioner's interpretation of key provisions of the Privacy Act. The Commissioner's Guidelines are not given any legislative status. However, the Guidelines may influence subsequent judicial interpretation of relevant provisions that are subject to guidance. It is interesting to note in this regard that in some cases the explanation of the intended operation of certain provisions of the amending Act that is given in the Explanatory Memorandum to the amending Act and also referred to in the Guidelines does not appear to conform to a plain reading of corresponding provisions of the amending Act. Issues of interpretation are therefore likely to arise.

2 Australian privacy framework and coverage

The use of 'personal information' (sometimes referred to as 'personally identifying information' or 'PI') in Australia is primarily regulated by the Privacy Act 1988. This is a federal Act administered by the Federal Attorney-General. The Privacy Commissioner is integrated within the Office of the Australian Information Commissioner (OAIC) (www.oaic.gov.au).

The amendments to the Privacy Act that commenced on 12 March 2014 substantially increase the level of federal privacy regulation and powers and sanctions of the federal enforcement agency. The following discussion focusses on the APPs as they will apply to private sector organisations: note that the rules applicable to government agencies differ in important matters of detail that are outside the scope of this review.

The Privacy Act is drafted in less prescriptive terms than European legislation. It does not use the European concepts of 'data owner', 'data controller' or 'data processor'. The Privacy Act does use other terms and concepts that are similarly used in other national privacy laws. However, the Privacy Act differs in varying respects to all other national privacy laws, including national laws in other APEC countries including Singapore, Malaysia and New Zealand. For this reason caution should be exercised when considering examples of regulatory action in other jurisdictions, even where the relevant terms used in the legislation appear to be similar. Also, privacy jurisprudence in other jurisdictions, particularly in the European Union, is often influenced by constitutional law or human

rights principles that do not affect consideration of Australian privacy law. European privacy regulation also places significant reliance upon use of standardised contractual terms and rulings as to the adequacy of levels of protection of privacy under particular foreign jurisdictions for cross-border data transfers. These concepts are not generally used in Australian privacy law.

Further complexities arise through the longevity of Australian privacy law when measured in internet time. Although the amendments to the Privacy Act commencing on 12 March 2014 are significant, these amendments were developed from an Australian Law Reform Commission (ALRC) review into the Privacy Act that was completed in May 2008. That review predated important technological and business developments including availability of tablet and mobile apps, broad adoption of social networking services, extensive use of data hosting services, delivery of software applications as a service (often provided from overseas and sometimes transient and indeterminate locations), extensive use of geo-location services, online behavioral advertising and 'big data' based customer data analytics. Each of these developments challenge traditional privacy concepts of territorial based regulation and informed user consent based upon privacy statements and privacy notices. In September 2013 the Privacy Commissioner developed a guide for app developers to embed better privacy practices in their products and services and to help developers operate in the Australian market in accordance to Australian privacy law. However, mobile and tablet apps were not considered in the ALRC review. The international rollout of apps and delivery of app based services creates fundamental difficulties in application of national privacy regulation such as the Australian Privacy Act. Compounding the problem, the Privacy Act has sketchy geographical and jurisdictional nexus provisions that are difficult to interpret and apply in relation to internet delivered services provided across national borders. Frequently, jurisdictional questions cannot be clearly answered and the laws of multiple jurisdictions must be applied.

The Privacy Act is intended to, at least partly, implement Australia's privacy obligations under the International Covenant on Civil and Political Rights and to give effect to the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. However, international law has had limited influence on the development of Australian privacy jurisprudence. Also, and as at January2014, there is no right of individuals in Australia conferred by international law or the Australian Constitution that protects an individual's seclusion or other 'rights' of privacy. Nor is there a common law or other general legal right of protection from invasion of privacy. Although some Australian court dicta supports the possibility of the development of a tortious cause of action for serious invasion of personal privacy, on current Australian law the availability of that right, and availability of practical and effective remedies to enforce it, is highly questionable. There has been an active debate in Australia

as to whether there should be a statutory cause of action for serious invasion of personal privacy and, if so, as to the appropriate remedies and enforcement mechanisms. That debate had been significantly influenced by concerns that investigative journalism could be significantly constrained by any private right of action in privacy. In June 2013, the then Australian Attorney-General commissioned the ALRC to conduct an inquiry into the protection of privacy in the digital era. The Terms of Reference require the ALRC to report by June 2014 and to make recommendations regarding, among other things, the legal design of a statutory cause of action for serious invasions of privacy, including legal thresholds; the effect of the implied freedom of political communication; jurisdiction; fault elements; proof of damages; defences; exemptions and access to justice. The ALRC's Discussion Paper, including its draft recommendations, is expected to be released in early March 2014.

Although private rights of action for privacy related acts or practices are currently limited, private rights of action may arise through recourse to other causes of action, including where an entity has engaged in misleading or deceptive conduct by failing to comply with the entity's privacy policy. This might lead to proceedings under section 18 of the Australian Consumer Law (Schedule 2 to the Competition and Consumer Act 2010) through private right of action or enforcement action by the Australian Competition and Consumer Commission (ACCC). The United States Federal Trade Commission (FTC) does not have any express jurisdiction to address privacy breaches, but the FTC has become an active privacy regulator through prosecution of alleged violations of section 5 of the U.S. Federal

Trade Commission Act or the FTC Act (15 USC 45), which bars unfair and deceptive acts and practices in or affecting commerce. This power has been used in law enforcement to require companies to live up to promises to consumers that they will safeguard their personal information and enabled the FTC to exact very substantial fines where companies fail to do so.

Practical remedies for Australians adversely affected by privacy invasive practices of businesses may also be available through the operation of binding APP codes and other binding sector-specific codes with privacy provisions. These include codes regulating broadcasting and the print media, the banking and financial services sectors and the provision of telecommunications services (including internet access services) to Australian consumers.

3 More detail about the federal Privacy Act

Under the Australian federal system, the Privacy Act applies to the handling of personal information by the Australian federal government and its agencies and the Australian Capital Territory (ACT) government and its agencies. The federal Privacy Act also governs the private sector, including corporations and other businesses, but (subject to important exceptions) only operates where annual Australian revenue of the Australian group business is greater than AU$3 million.

Organisations and agencies are collectively referred to as 'APP entities'. Many provisions of the Privacy Act apply to all APP entities, but some apply only to agencies, and some only to organisations.

The Privacy Act defines 'organisation' broadly to include an individual, body corporate, partnership, trust or any unincorporated association.

The APPs are arranged in the order of the personal information lifecycle, from collection, to use, to disclosure, to retention. They are not lengthy, but their interpretation can be complex. The Commissioner's new Guidelines as to their interpretation and operation of the APPs run to over two hundred pages. As already noted, some APPs draw distinctions between organisations and agencies, while otherwise applying to all APP entities. Some APPs require different and higher standards in relation to the sub-category of personal information that is sensitive personal information.

Subject to those qualifications, the coverage of the APPs is summarised below:

APP 1 — Open and transparent management of personal information

APP entities (that is, entities regulated by the Australian privacy laws) must manage personal information in an open and transparent way.

This includes having a clearly expressed and up to date APP privacy policy. Collection, use and retention of personal information should be minimised to that reasonably required as notified in a privacy policy or otherwise with a user's consent.

'Transparent' is not defined, but as used in the Australian Consumer Law a contractual term is 'transparent' if it is expressed in reasonably plain language, legible, presented clearly and readily available to the person affected by the term. The positive obligation for organisations to implement practices, procedures and systems to 'manage' personal information has been interpreted as requiring implementation of privacy assurance practices and procedures — sometimes called 'Privacy by Design' - into business processes and products.

APP 2 — Anonymity and pseudonymity

APP entities must give individuals the option of not identifying themselves, or of using a pseudonym. Limited exceptions apply.

APP 3 — Collection of solicited personal information

Outlines when an APP entity can collect personal information that is solicited by the entity.

APP 3 applies higher standards to the collection of 'sensitive' information, such as health information.

APP 4 — Dealing with unsolicited personal information

Outlines how APP entities must deal with unsolicited personal information.

APP 5 — Notification of the collection of personal information

Outlines when and in what circumstances an APP entity that collects personal information must notify an individual of certain matters.

APP 1 and APP 5 together set out quite prescriptively those things that need to be notified to an individual in relation to any collection of personal information about that individual.

Special requirements apply where personal information about an individual is collected from anyone

other than the affected individual.

APP 6 — Use or disclosure of personal information

Outlines the circumstances in which an APP entity may use or disclose personal information that it holds.

APP 7 — Direct marketing

An organisation may only use or disclose personal information for direct marketing purposes if certain conditions are met. Broadly, direct marketing:

- is use or disclosure of personal information to communicate directly with an individual to promote goods and services;
- may only be undertaken where an individual would reasonably expect it, such as with informed consent;
- must provide a prominent statement about a simple means to opt out;
- must be stopped when an individual opts-out.

APP 8 — Cross-border disclosure of personal information

Outlines the steps an APP entity must take to protect personal information before it is disclosed to any other entity (including related entities) overseas.

APP 9 — Adoption, use or disclosure of government related identifiers

Outlines the limited circumstances when an organisation may adopt a government related identifier of an individual as its own identifier, or use or disclose a government related identifier of an individual.

Examples of government related identifiers are divers licence numbers, Medicare numbers, Australian passport numbers and Centrelink reference numbers.

APP 10 — Quality of personal information

An APP entity must take reasonable steps to ensure the personal information it collects is accurate, up to date and complete. An entity must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure.

APP 11 — Security of personal information

An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure.

An entity has obligations to destroy or de-identify personal information in certain circumstances.

APP 12 — Access to personal information

An APP entity must provide access when an individual requests to be given access to personal information held about them by the entity.

Some limited, specific exceptions apply.

APP 13 — Correction of personal information

An APP entity must correct information held by it about an individual in response to a reasonable request by an affected individual.

Under the Privacy Act as amended from March 2014, industry groups or sectors may develop privacy codes of practice - so-called 'APP codes' - for review and possible registration by Office of the Australian Information Commissioner. If accepted for registration (and then in like manner to ACMA Codes) an APP Code becomes binding upon organisations within the industry sector specified in the Code. In other words, a Code once registered binds not only initial or later signatories to the Code, but also binds organisations within the industry sector to which the Office of the Australian Information Commissioner designates the Code applies. To date, only a small number of such codes have been approved, including in particular the Credit Reporting Privacy Code issued under the Privacy Act. It is expected that other industry codes will be now developed and registered with the OAIC.

4 Other privacy laws

The Privacy Act does not regulate the handling of personal information by Australian state or territory governments and their agencies, except to a very limited extent. Some Australian states and territories have enacted privacy statutes containing data protection principles broadly similar to the federal privacy principles that, in general, are enforced by State officers styled ‘Privacy Commissioners’ or similar. These state and territory laws govern acts and practices of the respective Australian state or territory government and its agencies. In some cases these statutes also govern handling by the private sector on behalf of the government or its agency of personal information collected by the government or its agencies. In addition, some Australian state and territory jurisdictions have legislation that extends to private sector handling of particular categories of sensitive personal

information collected directly by the private sector. One example is the State of Victoria’s Health Records Act 2001, which regulates health related Information about individuals that is collected in the State of Victoria. Regulation of workplace surveillance and surveillance in public places, use of tracking devices, geo-tracking and recording technologies is currently principally state based and diverse.

Certain criminal laws also provide protection for individuals from intrusions about their right to seclusion, including in particular laws on unauthorised access to computer systems, electronic stalking and harassment, and unauthorised audio-visual capture of sexual activity, also regulate and protect privacy. Handling of telecommunications customer data is subject to sector specific regulation, principally through the Telecommunications Act 1997, a federal Act. The Telecommunications Act 1997 is administered by the Federal Minister for Communications and by the Australian Communications and Media Authority (ACMA). The ACMA also administers Codes registered under

the Telecommunications Act 1997 that, once registered by the ACMA, become binding upon the section of the telecommunications industry to which the code relates. The Telecommunications Consumer Protection Code 2012 is an important legally binding instrument that regulates the handling of customer data by Australian telecommunications carriers and carriage service providers. The federal Telecommunications (Interception and Access) Act 1979, administered by the Federal Attorney-General, regulates interception of telecommunications (including email) traffic and access to stored communications held on email and other servers in Australia that are controlled by Australian licensed telecommunications carriers.

There are other industry specific codes that include privacy protective provisions that have varying levels of enforceability and sanctions. Perhaps the most important are the broadcasting codes of practice administered by the ACMA which may be contravened where a television or radio broadcaster broadcasts material that is a serious invasion of an individual's privacy. The Australian Press Council administers a code of practice as to print media and its associated electronic outlets, which is contravened where a Council member publishes material that is a serious invasion of an individual's privacy. Other industry sectors deal with customer privacy in industry codes, including the Banking Industry Code of Practice and the Insurance Industry Code of Practice.

There are no cookie-specific laws such as those in the European Union. The use of cookies requires appropriate notification to internet users whenever personal information is collected through the use of those cookies.

The Australian Guideline for Online Behavioural Advertising is a self-regulatory guideline for third party online behavioural (interactive) advertising. The guideline regulates sharing of information between signatories to the guideline and third parties that would enable third parties to serve behavioural advertising to an internet user. In such a circumstance user consent and provision of a ready means for an individual to opt-out is required, regardless of whether personal information is disclosed by code signatory to the third party and regardless of whether cookies or other tracking technologies are used. The guideline prescribes the relevant requirements.

5 Enforcement of the Privacy Act

As already noted, the Privacy Act is administered by the Commissioner within the OAIC. The OAIC is responsible for enforcing compliance with the Privacy Act and reviewing proposed privacy codes. This involves investigating instances of non-compliance by agencies and organisations and prescribing remedies to redress non-compliance. The terms 'Privacy Commissioner' and 'OAIC' are often used interchangeably.

There are criminal penalties under the Privacy Act for unauthorised access to and disclosure of credit reporting PI. If, during an investigation, the Commissioner forms the opinion that these offences (and

certain others under other Acts) may have been committed, he or she must refer the matter to the Australian federal police.

Criminal sanctions also apply to the unauthorised disclosure of PI during an emergency or disaster situation. The Australian federal police would investigate such offences.

The Commissioner has the power to investigate on his or her own motion, or in response to a complaint (from an individual or a class), acts and practices of organisations that may breach the APPs. In conducting investigations, the Commissioner must follow a prescribed process. The Commissioner can require the production of documents and information, and may also require people to appear and answer questions.

The Commissioner may make a non-binding determination following investigation of a complaint where there has been a breach of the APPs. The Commissioner may determine that the conduct must not be repeated; that the agency or organisation must take action to redress the loss or damage caused; or that the complainant is entitled to a specified amount of compensation. The Commissioner may also dismiss the complaint or decide to take no further action. If it is necessary to enforce the Commissioner's determination, action must be taken in the Federal Courts.

From March 2014, the Commissioner also has a power to seek a Court injunction against a person engaging in conduct that may contravene the Privacy Act, to obtain enforceable undertakings by a person that has breached the Privacy Act, and to seek the making by a federal court of civil penalty orders where there is either a serious or repeated interference with the privacy of an individual. A civil penalty order may require a body corporate to pay up to $1.7 million. A civil penalty is a pecuniary penalty imposed by a court according to civil (as opposed to criminal) processes. It is expected that the new power to accept court enforceable undertakings from organisations will be used to gain agreement from organisations that experience data breaches to implement privacy compliance programmes and change existing information security and information handling practices. This power to accept court enforceable undertakings is similar to that enjoyed, and frequently used, by the ACCC under the Competition and Consumer Act 2010 and by the ACMA under the Spam Act 2003 and the Do Not Call Register Act 2006.

The Commissioner's new enforcement powers are summarised in the following diagram:

In many cases there is parallel and potentially concurrent operation of federal law, state and territory law and industry codes of practice. This sometimes leads to simultaneous and sometimes coordinated enforcement action by multiple regulators, such as the OAIC and the ACMA. This has been the case on multiple occasions in relation to misuse of telecommunications customer data. Overlap may also arise in respect of other sectors. For example, a health PI data breach in Victoria may be handled by both the Victorian Health Services Commissioner and the Australian Privacy Commissioner.

6 Exempt sectors and institutions

The Privacy Act does not apply to the collection, holding, use, disclosure or transfer of PI by an individual for the purposes of, or in connection with, the individual's personal, family or household affairs.

While the Privacy Act applies to many private and public sector organisations and agencies, certain entities are excluded from the Act's coverage. These include small business operators (generally,

operators of businesses with an annual Australian turnover (determined on a corporate group basis) of less than A$3 million), registered political parties, organisations that are individuals acting in a non-business capacity, organisations acting under a state contract, employer organisations acting in respect of employee records and the Australian intelligence agencies.

The Privacy Act deals with employee records of public sector and private sector employees differently. The handling of personal information by a private sector employer is exempt from the Privacy Act if it is directly related to a current or former employment relationship or an employee record. The effect is that a private sector employer does not need to comply with the APPs when it handles current and past employee records, or grant a current or former access to the employee record about them. However, the employee records exemption relates to private sector organisations only: Australian, ACT and Norfolk Island government employee records are covered by the Privacy Act.

An act or practice is not an interference with privacy if it consists of the collection or disclosure of personal information by a body corporate from or to a 'related body corporate'. Before an organisation can rely on this exemption to disclose (non-sensitive) personal information to other related companies, it must take reasonable steps to ensure that the individual knows that the organisation has collected the information, the use that will be made of the information and the types of organisations to which the information is usually disclosed. In addition, although related companies may share personal information, the handling of that information is still subject to the APPs in all other respects. For example, each company within the group of related companies must only use the information for the primary purpose for which it was originally collected, and may only use the personal information for a secondary purpose permitted for the collecting organisation.

This partial exemption for related bodies corporate also does not apply in a range of circumstances, including (but not only) the collection or disclosure of 'sensitive information'; the collection of personal information from an entity that is exempt from the Privacy Act; where the company is a contractor under a Commonwealth contract and; the collection or disclosure of personal information from or to the related company is contrary to a contractual provision; and where the collection of personal information is for the purpose of meeting an obligation under the contract and the disclosure is for direct marketing purposes.

The journalistic activities of media organisations are exempt from the Privacy Act to the extent that such organisations publicly commit to observe published privacy standards (such as industry codes of practice). Currently, both print and broadcast media in Australia are required to adhere to principles and industry codes of practice that contain privacy standards applicable to journalistic activities, respectively the Australian Press Council's Statement of Privacy Principles and a number of broadcast television and radio Industry Codes of Practice administered by the ACMA. The area of media and convergent services regulation, including the effectiveness of media self-regulatory schemes, has been the subject of considerable controversy and a number of government reviews over recent years. It is likely that privacy regulation in the media sector will significantly change in the foreseeable future.

Further privacy reform, including as to the coverage exemptions, is likely. The ALRC recommended the repeal of the coverage exemptions for small business, registered political parties and employee records. The previous Australian (Labor) government undertook to consider these recommendations: it is unclear whether the current Australian coalition government will further consider the ALRC's recommendations.

7 Communications, surveillance, marketing and other laws

As noted above, the Privacy Act does not expressly cover the interception of electronic communications or the monitoring and electronic surveillance of individuals. There are a number of subject matter specific federal and state laws governing telecommunications interception (including

access to stored communications such as emails), employee, video and workplace surveillance, and use of recording devices, listening devices and tracking devices.

Electronic marketing is either regulated through subject matter specific federal laws governing spam and unsolicited marketing calls or by new APP 7 which regulates use or disclosure of PI for the purpose of direct marketing activities. APP 7 will not apply to the extent that any of the federal spam and unsolicited marketing calls laws apply to an organisation. Generally, organisations may only use or disclose personal information for direct marketing purposes where the individual has either consented to their personal information being used for direct marketing, or has a reasonable expectation that their personal information will be used for this purpose, and conditions relating to opt-out mechanisms are met. APP 7 generally prohibits the use and disclosure of PI for the purpose of direct marketing except in limited circumstances and then under specific conditions and applies more onerous obligations on organisations that direct market to non-existing customers.

Laws dealing with interception, monitoring and surveillance, and electronic marketing include the following:

- Spam Act 2003 (Cth), which deals with the sending of unsolicited commercial electronic messages, including emails and SMS;
- Do Not Call Register Act 2006 (Cth), regulating unsolicited commercial calling to telephone numbers listed on the national Do Not Call Register;
- eMarketing Code of Practice, which contains rules and guidelines for the sending of commercial electronic messages. The Code is given legal effect by registration of that Code with the ACMA;
- Telecommunications (Interception and Access) Act 1979 (Cth), which among other things, regulates the interception of, and access to, stored communications by law enforcement agencies;
- a range of federal and state and territory statutes governing the use of listening devices and workplace surveillance; and
- a more limited range of federal and state and territory statutes governing the use of unauthorised video surveillance;
- state and federal criminal law provisions dealing with unauthorised access to computer systems; and
- the Australian Guideline for Third Party Online Behavioural Advertising.

The Spam Act prohibits 'unsolicited commercial electronic messages' with an 'Australian link' from being sent or caused to be sent. Commercial electronic messages may only be sent with an individual's consent (express or implied in certain circumstances) and where the message contains

accurate sender identification and a functional unsubscribe facility.

The Spam Act defines a 'commercial electronic message' as any electronic message (including e-mail, SMS, multimedia messages, instant messages or any other direct electronic messaging) where having regard to:

- the content of the message;
- the way in which the message is presented; and

- content that can be accessed by following any links, phone numbers or contact information in the message,

it could be considered that a purpose, or one of the purposes, of the message is to:

- offer, advertise or promote the supply of goods, services, land or business or investment opportunities;
- advertise or promote a supplier of goods, services, land or a provider of business or investment opportunities; or
- assist or enable a person to dishonestly obtain property, commercial advantage or other gain from another person.

Any electronic message that passes this test of commerciality is caught by the Spam Act (subject to certain exceptions). Commerciality may be a secondary purpose and the message is still caught: for example, a message that is mainly factual or useful information, but then has some marketing or promotional content.

A message has an 'Australian link' if it originates or was commissioned in Australia, or originates overseas, but was sent to an address accessed in Australia. The Spam Act expressly includes e-mails, SMS, instant messages and MMS. The Spam Act expressly excludes voice calls made using any technology and including synthetic or recorded calls (such as robocalls).

Voice calls, including synthetic or recorded calls (such as robocalls), are separately regulated under a 'do not call' regulatory framework established under the Do Not Call Register Act 2006 and associated legislation and instruments, including the important Telecommunications (Do Not Call Register) (Telemarketing and Research Calls) Industry Standard 2007.

Marketing faxes are regulated under the Do Not Call Register Act 2006. This Act provides an 'opt-out' framework for these forms of marketing. Unsolicited telemarketing calls or faxes must not be made to an Australian number registered on the Do Not Call -Register.

The Spam Act 2003 and the Do Not Call Register Act 2006 are administered by the ACMA. Extensive material as to the operation of these statutes and enforcement activity by the ACMA is available at www.acma.gov.au.

State and territory statutes dealing with interception, monitoring and surveillance laws vary substantially, both in scope of coverage and drafting. In particular, many computer crime and unauthorised access and surveillance provisions were not drafted with regard to current applications of the internet and mobile devices and are therefore difficult to interpret and apply.

Other specific data protection rules in areas related to privacy include:

- Part 13 of the Telecommunications Act 1997 (Cth), which imposes restrictions on the use and disclosure of telecommunications and communications-related data;
- state and territory privacy legislation, applying to personal information held by government agencies and, in some cases, health information and records (for example, the Privacy and Personal Information Protection Act 1988 (NSW));
- the Healthcare Identifiers Act 2010 (Cth), regulating (among other things) the use and disclosure of healthcare identifiers;

- the Data-matching Program (Assistance and Tax) Act 1990 (Cth), which regulates federal government data-matching using tax file numbers;
- the Personally Controlled Electronic Health Records Act 2012 (Cth), which provides strict controls on the collection, use and disclosure of health information included in an individual's eHealth record; and
- federal and state/territory freedom of information legislation applying to information held by government agencies.

There is no legislation in Australia similar to the US Federal Children's Online Privacy Protection Act of 1998 (COPPA), although COPPA principles are commonly applied in Australia as a matter of good corporate practice.

8 Personably identifying information

Generally, the Privacy Act covers all processing (in Australian terms, itself a 'use') or use of personal information.

The Act makes no express distinction between entities that control or own personal information, and those that provide services to owners (except in the case of contracted service providers to public-sector agencies). All such entities are regulated as APP entities in respect of their handling of personal information.

The definition of 'personal information' from March 2014 extends to information or an opinion about an individual who is reasonably identifiable, whether or not the information or opinion is recorded in a material form (this includes information communicated verbally) and regardless of whether that identification or re-identification is practicable from the information itself or in combination with or reference to other information.

Personal information will therefore include information about an individual whether collected or made available in a personal or business context and regardless of whether that information is in the public

domain and the subject individual is specifically identified or consented for that information to enter the public domain.

Personal information remains such while ever identification or re-identification of an individual is 'practicable' either from the information itself or by reference to that information in combination with or by reference to other information. Privacy regulation operates up to the point at which personal information is transformed such that any risk that the information might either of itself or in combination with other information enable an individual to be identifiable becomes effectively impracticable. That transformation might be through aggregation or anonymisation of the personal information. Many organisations maintain multiple transaction databases, some of which may include personal information and some of which may include transaction data that does not identify a particular individual undertaking a transaction. These databases may be partitioned so that the non-identifying transactional database is not matched against the databases containing personal information. Partitioning of databases within organisations will be ineffective to allow non-identifying transactional data to be used without complying with the rules that relate to use of personal information, wherever there is any way in which an individual could be matched and tied to non-identifying transaction data, because the individual remains 'reasonably identifiable'. The Privacy Commissioner's February 2014 Guidelines put it this way:

> B.87 Whether a person is 'reasonably identifiable' is an objective test that has practical regard to the context in which the issue arises. Even though it may be technically possible to identify an individual from information, if doing so is so impractical that there is almost no likelihood of it

> occurring, the information would not generally be regarded as 'personal information'. An individual may not be reasonably identifiable if the steps required to do so are excessively time-consuming or costly in all the circumstances.
>
> B.88 Where it is unclear whether an individual is 'reasonably identifiable', an APP entity should err on the side of caution and treat the information as personal information.

This view reflects regulatory guidance in some jurisdictions to the effect that determination as to whether information is 'personal information' is to be made having regard to all relevant circumstances as to possible re-identification by any reasonably contemplated recipient, or as it is sometimes put, to be made 'in the round', rather than having regard to whether the information was passed to the first recipient in apparently de-identified form. In assessing the risk of re-identification, regulatory guidance in some jurisdictions suggests that risk management strategies — or as it is sometimes put, technical, operational and contractual safeguards — are to be taken into account. The United Kingdom regulator suggest a 'motivated intruder' test: this test considers whether a reasonably competent motivated person with no specialist skills would be able to identify the data or information, having access to resources such as the internet and all public documents and making reasonable enquiries to gain more information.

9 Extraterritoriality

The Privacy Act applies to all acts or practices within Australia in respect of personal information about individuals wherever those individuals may reside.

Accordingly, personal information of persons outside Australia that is held on servers located within Australia is regulated by the Act.

The Act extends to any use outside Australia or disclosure from Australia of personal information that has been collected within Australia, although the extraterritorial application of the Act in this area is subject to some uncertainty.

The Act also applies to an act or practice wherever done outside Australia by an agency (broadly, an Australian federal government entity).

The Act also applies in relation to an act or practice outside Australia to an organisation or small business operator wherever that organisation or small business operator has a relevant 'Australian link'. A small business operator is regulated in relation to an act or practice outside Australia, but only to the extent similarly regulated in Australia.

In general, corporations incorporated in Australia and Australian incorporated or constituted bodies are deemed to have an Australian link.

Corporations and other bodies and agencies that do not fall into the above categories - broadly, any foreign corporation or body - will be regulated where (1) the organisation carries on business in Australia, and (2) the personal information was collected or held by the organisation in Australia, either before or at the time of the act or practice.

The collection of personal information 'in Australia' includes the collection of personal information from an individual who is physically within the borders of Australia, or an external territory, by an overseas entity. The Explanatory Memorandum to the Privacy Amendment (Enhancing Privacy Protection) Bill 2012 states that a collection is taken to have occurred 'in Australia' where an individual is physically located in Australia or an external Territory and personal information is collected from that individual via a website and the website is hosted outside of Australia and owned by a foreign company that is based outside of Australia and that is not incorporated in Australia'. The Explanatory Memorandum

goes on to state that for the operation of the Act, entities such as those described in the last sentence who have an online presence (but no physical presence in Australia) and collect personal information from people who are physically in Australia, carry on a 'business in Australia or an external Territory'. However, this interpretation is not supported by a plain reading of the Act and prior Australian jurisprudence (as to other statutory provisions) concerning carrying on business in Australia. Accordingly, the operation of the Privacy Act in this scenario (without other factors indicating business presence in Australia) should be considered currently uncertain and potentially contentious.

An overseas act or practice (that takes place outside Australia and its external Territories) act or practice will not breach the APPs, an approved APP Code, or interfere with an individual's privacy, if the act or practice is required by an applicable foreign law. However, a similar act or practice within Australia pursuant to compulsion of an applicable foreign law is not excused from breach of the APPs or an approved APP Code, or from being an interference with an individual's privacy.

It is also important to note that APP 8, which deals with the cross-border disclosure of personal information from Australia to outside Australia, is not limited in its application by the nationality of the individual whose PI is the subject of the transfer. In other words, APP 8 will apply to a cross-border disclosure of personal information collected in Australia, irrespective of whether the information relates

to an Australian citizen or Australian resident or not.

10 Regulation of collection, use and disclosure of PI

The Privacy Act requires that the collection, use and disclosure of personal information must be justified on specific grounds.

An organisation must have an APP privacy policy that contains specified information, including the kinds of personal information it collects, how an individual may complain about a breach of the APPs, and whether the organisation is likely to disclose information to overseas recipients.

An organisation also needs to take reasonable steps to make its APP privacy policy available free of charge and in an appropriate form.

APP 1 also introduces a positive obligation for organisations to implement practices, procedures and systems that will ensure compliance with the APPs and any registered APP codes. APP 1 requires organisations to have ongoing practices and policies in place to ensure that they manage personal information in an open and transparent way. 'Transparent' is not defined, but as used in the Australian Consumer Law a contractual term is 'transparent' if it is expressed in reasonably plain language, legible, presented clearly and readily available to the person affected by the term. The positive obligation for organisations to implement practices, procedures and systems has been suggested to require implementation of privacy assurance practices and procedures — so-called 'Privacy by Design' principles - into business processes and products.

APP 3 outlines when and how an organisation may collect personal and sensitive information that it solicits from an individual or another entity. An organisation must not collect personal information (other than sensitive information) unless the information is reasonably necessary for one or more of the organisation's functions or activities.

APP 3 clarifies that, unless an exception applies, sensitive information must only be collected with an individual's consent if the collection is also reasonably necessary for one or more of the organisation's functions or activities.

An organisation must only collect personal information from the individual, unless it is unreasonable or impracticable to do so.

APP 4 creates obligations in relation to the receipt of personal information which is not solicited. Where an organisation receives unsolicited personal information, it must determine whether it would have been permitted to collect the information under APP 3. If so, APPs 5 to 13 will apply to that information. If the information could not have been collected under APP 3, the organisation must destroy or de-identify that information as soon as practicable, but only if it is lawful and reasonable to do so.

APP 5 specifies certain matters about which an organisation must generally make an individual aware, at the time, or as soon as practicable after, the organisation collects their personal information.

In addition to other matters listed in APPs 1.4 and 5.2, APP 5 requires organisations to notify individuals about the access, correction and complaints processes in their APP privacy policies, and also the location of any likely overseas recipients of individuals' information.

APP 6 outlines the circumstances in which an organisation may use or disclose the personal information that it holds about an individual. If an organisation collects personal information about an individual for a particular purpose (the primary purpose), it must not use or disclose the information for another purpose (the secondary purpose) unless the individual consents to the use or disclosure, or another exception applies.

Additional protections apply to the collection, use and disclosure of a subcategory of PI called 'sensitive information', which the Privacy Act defines as information or an opinion about an individual's:

- racial or ethnic origin;
- political opinions;
- membership of a political association;
- religious beliefs or affiliations;
- philosophical beliefs;
- membership of a professional or trade association;
- membership of a trade union;
- sexual orientation or practices; or
- criminal record,

which is also personal information; and

- health information about an individual;
- genetic information about an individual that is not otherwise health information;
- biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or
- biometric templates.

An organisation must not collect an individual's sensitive information unless an exception applies. Sensitive information may be collected about an individual with consent and if the information is reasonably necessary for one or more of the organisations activities or functions. Further, an organisation may collect sensitive information if required or authorised by or under an Australian law or a court/tribunal order or in certain permitted health situations, such as where the entity reasonably believes that the collection is necessary to lessen or prevent a serious threat to the life, health or safety of any individual or to public health or safety.

The Privacy Act also contains special provisions that apply to PI included in individuals' credit information files or in credit reports, including information about an individual's repayment history. These provisions also provide for consumer protection in relation to processes dealing with notification, data quality, access and correction and complaints.

The Act also provides for the making of guidelines by the Commissioner concerning the collection, storage, use and security of tax file number information. Compliance with the Tax File Number Guidelines is mandatory for all tax file number recipients.

APP 6 (Use and disclosure) generally restricts the use and disclosure of PI to the primary purpose for its collection or related secondary purposes within the exceptions discussed above. A user may consent to other uses or disclosures.

Further restrictions on the disclosure of credit-related PI are set out in the credit reporting provisions of the Act. Such disclosure restrictions include the following:

- a credit reporting body must not disclose personal information contained in an individual's credit information file to a third party unless one of the specified exceptions applies (such as where the information is contained in a credit report given to a credit provider for the purpose of assessing an application for credit by the individual); and
- a credit provider must not disclose any PI in a credit report to a third party for any purpose (subject again to specified exceptions).

The Act also imposes specific restrictions on the transfer of PI outside Australia, as discussed below in section 20 (Cross-border transfer).

11 'Openness' and Notification

APPs 1 and 5 impose 'openness' requirements in relation to collection of personal information.

An APP entity must take reasonable steps to notify an individual, or otherwise ensure that the individual is aware, that its APP privacy policy contains information about how to access and seek correction of personal information, and information about the organisation's complaints process; and whether it is likely to disclose an individual's personal information to overseas recipients and, if it is practicable, to specify the countries in which those recipients are likely to be located. If it is not practicable to specify the countries in the notification, the organisation may make the individual aware of them in another way.

Notification obligations arise under the Privacy Act at the point of collection of PI by an organisation, whether collected directly from the individual or obtained from a third party. If the organisation collects the personal information from someone other than the individual, or the individual may not be aware that the organisation has collected the personal information, it must also take reasonable steps to notify an individual, or otherwise ensure that the individual is aware:

- that the organisation collects or has collected the information, and
- of the circumstances of that collection (APP 5.2(b)).

Some notification requirements may be addressed through the publication of a privacy policy. Specifically, APP 1.4 requires APP entities collecting PI to specify the following matters in their privacy policy:

- the kinds of personal information that the entity collects and holds;
- how the entity collects and holds personal information;
- the purposes for which the entity collects, holds, uses and discloses personal information;
- how an individual may access personal information about the individual that is held by the entity and seek the correction of such information;
- how an individual may complain about a breach of the Australian Privacy Principles, or a registered APP code (if any) that binds the entity, and how the entity will deal with such a complaint;
- whether the entity is likely to disclose personal information to overseas recipients
- if the entity is likely to disclose personal information to overseas recipients—the countries in which such recipients are likely to be located if it is practicable to specify those countries in the policy.

More specific notification requirements are stated in APP 5. At or before the time or, if that is not practicable, as soon as practicable after, an APP entity collects personal information about an individual, the entity must take such steps as are reasonable in the circumstances to notify the individual of such matters referred to in subclause 5.2; or to otherwise ensure that the individual is aware of any such matters. The matters referred to in subclause 5.2 are:

- the identity and contact details of the APP entity;
- if the APP entity collects the personal information from someone other than the individual; or the individual may not be aware that the APP entity has collected the personal information, the fact that the entity collects or has collected the information and the circumstances of that collection;
- if the collection of the personal information is required or specifically authorised by Australian law or court order, details about that;
- the purposes for which the APP entity collects the personal information;
- the main consequences (if any) for the individual if all or some of the personal information is not collected by the APP entity;
- any other person, or the types of persons, to which the APP entity usually discloses personal information of the kind collected by the entity;
- that the APP privacy policy of the APP entity contains information about how the individual may access the personal information about the individual that is held by the entity and seek the correction of such information;

- that the APP privacy policy of the APP entity contains information about how the individual may complain about a breach of the APPs, or a registered APP code (if any) that binds the entity, and how the entity will deal with such a complaint;

- whether the APP entity is likely to disclose the personal information to overseas recipients;

- if the APP entity is likely to disclose the personal information to overseas recipients—the countries in which such recipients are likely to be located if it is practicable to specify those countries in the notification or to otherwise make the individual aware of them.

Use or disclosure of personal information for a purpose other than the primary purpose of collection (being a 'secondary purpose') is permitted under specific exceptions where that secondary use or disclosure is:

- required or authorised by or under an Australian law or a court order;

- necessary to lessen or prevent a serious threat to any individual's life, health or safety, or to public health or safety, and it is unreasonable or impracticable to obtain the consent of the individual;

- necessary in order for an organisation to take appropriate action in relation to a reasonable suspicion of unlawful activity, or misconduct of a serious nature, that relates to the entity's functions or activities. APP 6.2(e) also permits the use or disclosure of personal information for a secondary purpose to an enforcement body for one or more enforcement related activities;

- in the conduct of surveillance activities, intelligence gathering activities or monitoring activities, by a law enforcement agency;

- the conduct of protective (for example, in relation to children) or custodial activities;

- to assist any APP entity, body or person to locate a person who has been reported as missing (where the entity reasonably believes that this use or disclosure is reasonably necessary, and where that use or disclosure complies with rules made by the Commissioner);

- for the establishment, exercise or defence of a legal or equitable claim; and

- for the purposes of a confidential alternative dispute resolution process.

Generally notification is required wherever a use or disclosure of personal information is made, unless a specific exception applies.

12 Control of use

There are a number of provisions in the Privacy Act which directly, or indirectly, enable individuals to exercise a degree of choice or control over use of their PI by organisations.

For example:

- APP 1 (Openness and transparency), which requires organisations to have ongoing practices and policies in place to ensure that they manage personal information in an open and transparent way;

- APP 2 (Anonymity and pseudonymity), which requires that an organisation provide individuals with the option of dealing with it using a pseudonym or anonymously. Both requirements are subject to certain limited exceptions, including where it is impracticable for the organisation to deal with an individual who has not identified themselves, or where the law or a court/tribunal order requires or authorises the organisation to deal with individuals who have identified themselves;

- APP 3 (Collection of solicited personal information), which clarifies that, unless an exception applies, sensitive information must only be collected with an individual's consent and if the collection is also reasonably necessary for one or more of the organisation's functions or activities;

- APP 5 (Notification), which requires organisations to notify individuals about the access, correction and complaints processes in their APP privacy policies, and also the location of any likely overseas recipients of individuals' information;

- APP 7 (Direct marketing), which requires the availability of opt-out mechanisms in relation to direct marketing;

- APP 12 (Access), which requires an organisation to give an individual access to the personal information that it holds about that individual, unless an exception applies. There is a new express requirement for organisations to respond to requests for access within a reasonable period. In addition, organisations must give access in the manner requested by the individual if it is reasonable to do so. If an organisation decides not to give an individual access, it must generally provide written reasons for the refusal and information about the mechanisms available to complain about the refusal;

- APP 13 (Correction), which requires an organisation to take reasonable steps to correct personal information to ensure that, having regard to a purpose for which it is held, it is accurate, up-to-date, complete, relevant and not misleading, if either the organisation is satisfied that it needs to be corrected, or an individual requests that their personal information be corrected. Organisations generally need to notify other APP entities that have been provided with the personal information of any correction, if that notification is requested by the individual.

13 Data accuracy

APP 10 (Integrity) requires an organisation to take reasonable steps to ensure that the personal information that it collects is accurate, up-to-date and complete,

In relation to use and disclosure, the APP 10 requirement is that an organisation will need to take reasonable steps to ensure that the personal information is relevant (in addition to being accurate, up-to-date, and complete), having regard to the purpose of that use or disclosure.

APP 13 (Correction) requires an organisation to take reasonable steps to correct personal information

to ensure that, having regard to a purpose for which it is held, it is accurate, up-to-date, complete, relevant and not misleading, if either the organisation is satisfied that it needs to be corrected, or an individual requests that their personal information be corrected. Organisations generally need to notify other APP entities that have been provided with the personal information of any correction, if that notification is requested by the individual.

14 Amount and duration of data holding

There are no express restrictions as to the quantity of PI an organisation may collect or hold, but organisations are prohibited from collecting and holding PI unless the information is reasonably necessary for one or more of the organisation's functions or activities.

In addition, where the personal information is sensitive information, organisations are prohibited from collecting and holding that sensitive information unless the individual consents and the information is reasonably necessary for one or more of the organisation's functions or activities or if an exception applies.

APP 11.2 requires an APP entity to take reasonable steps to destroy or de-identify personal information if the organisation no longer needs it for any for which it may be used or disclosed in accordance with the APPs. There are two exceptions to this requirement: if the personal information is contained in a Commonwealth record, or if the organisation is required by or under an Australian law or a court order to retain the information.

15 Finality principle

European privacy lawyers sometimes refer to a 'finality principle', to the effect that use and disclosure of personal information is limited by the purposes for which it was originally collected (subject to various exceptions). The concept is that organisations cannot change their minds about the uses they (or others) wish to make of personal information, after the event of collection.

The 'finality principle' is partially reflected in APP 6 (Use or disclosure). If an APP entity holds personal information about an individual that was collected for a particular purpose (the primary purpose), the entity must not use or disclose the information for another purpose (the secondary purpose) unless the individual has consented to the use or disclosure of the information; or an exception in subclause 6.2 or 6.3 applies.

Exceptions include:

- the individual would reasonably expect the APP entity to use or disclose the information for the secondary purpose and the secondary purpose is, if the information is sensitive information, directly related to the primary purpose; or if the information is not sensitive information, related to the primary purpose;
- the use or disclosure of the information is required or authorised by or under an Australian law or a court order;
- the use or disclosure of the information is necessary to lessen or prevent a serious threat to any individual's life, health or safety, or to public health or safety, and it is unreasonable or impracticable to obtain the consent of the individual;
- the use or disclosure of the information is necessary in order for an organisation to take appropriate action in relation to a reasonable suspicion of unlawful activity, or misconduct of a serious nature, that relates to the entity's functions or activities; or
- the individual has consented to the use or disclosure.

An APP entity may also use or disclose personal information for the secondary purpose of direct marketing subject to the prescriptive requirements of APP 7.

16 Data security and notification of data breaches

APP 11 (Security) requires organisations to take reasonable steps to protect PI from misuse, interference and loss and unauthorised access, modification or disclosure. When PI is no longer needed for an authorised purpose by an organisation, it must take reasonable steps to destroy or permanently de-identify it.

Reasonable steps in relation to protection of PI will vary with the circumstances. Relevant circumstances include (by way of non-exhaustive examples) how sensitive the PI is, how it is stored (e.g. paper or electronically), the likely harm to the data subject if a breach occurred and the size of the organisation. Similarly, destruction or de-identification processes will vary. In any event, PI should be destroyed securely and de-identified such that the data subject's identity is no longer reasonably ascertainable from the PI.

In April 2013, the OAIC published a guide to information security which discusses some of the circumstances that the OAIC takes into account when assessing the reasonableness of the steps taken by entities to ensure information is kept secure. This guide presents a set of non-exhaustive steps and strategies that may be reasonable for an entity to take in order to secure personal information. The OAIC has stated that the Commissioner will refer to this guide when assessing an entity's compliance with security obligations in the Privacy Act.

The Privacy Act does not presently impose obligations on agencies or organisations to notify either the OAIC, or the individual concerned, of security breaches involving personal information.

However, the OAIC recommends notification in its guidelines on this area 'Data Breach Notification: A guide to handling personal information security breaches, April 2012'. These guidelines are generally followed by corporations in Australia.

The ALRC recommended the introduction of a mandatory data breach notification scheme in its 2008 report, 'For Your Information: Australian Privacy Law and Practice'. In 2013, the then federal government introduced the Privacy Amendment (Privacy Alerts) Bill 2013. This Bill had not been passed by both Houses of the Federal Parliament when the Parliament was prorogued and accordingly lapsed. If enacted, this Bill would have built upon the OAIC's scheme of voluntary notification of serious data breaches by entities, as set out in the OAIC's guidelines. The Bill proposed a high threshold based on a reasonable belief by the entity concerned that the data breach is sufficiently serious to pose a real risk of serious harm to affected individuals. In the event of such a breach, the provisions of the Bill, if enacted, would have required the entity to notify affected individuals and the Information Commissioner as soon as practicable. The provisions of the Bill would require that the data breach notice include:

- the identity and contact details of the entity;
- a description of the breach;
- the kinds of personal information concerned;
- recommendations about the steps that individuals should take in response to the breach; and
- any other information specified in any made regulations under the Bill (if enacted).

As at January 2014, it was not clear whether the Coalition Government would re-introduce data breach notification legislation.

17 Data protection officer

Australia has no mandatory requirement to appoint a data protection officer.

It is becoming more common for major corporations to appoint a privacy professional, generally working within a legal or regulatory compliance team. However, there is no legal obligation to do so.

18 Record keeping

There is no general requirement as to record keeping. However, the Privacy Act does require an organisation to keep a written note of any use or disclosure of PI where the organisation reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.

Written notes must also be made in relation to certain uses or disclosures of credit related PI, including the use and disclosure of such information for direct marketing pre-screening assessments.

Further, reasonable steps under APP 11 (Security) may require certain processes to be established, depending on the circumstances.

Some Australian states require owners of health-related PI to keep records of when this type of PI is deleted or disposed of.

19 Access

If an APP entity holds personal information about an individual, the entity must, on request by the individual, give the individual access to the information (APP 12 (Access)).

Exceptions apply, as outlined below.

An APP entity's privacy policy should include information about how an individual may access personal information about the individual that is held by the entity and seek the correction of such information (APP 1.4(d)).

An APP entity must respond to a request for access to the personal information if the entity is an agency, within 30 days after the request is made; or if the entity is an organisation, within a reasonable period after the request is made; and give access to the information in the manner requested by the individual, if it is reasonable and practicable to do so.

Exceptions applicable to organisations include where:

- the entity reasonably believes that giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety;
- giving access would have an unreasonable impact on the privacy of other individuals;
- the request for access is frivolous or vexatious;
- the information relates to existing or anticipated legal proceedings between the entity and the individual, and would not be accessible by the process of discovery in those proceedings;

- giving access would reveal the intentions of the entity in relation to negotiations with the individual in such a way as to prejudice those negotiations;
- giving access would be unlawful;
- denying access is required or authorised by or under an Australian law or a court order;
- the entity has reason to suspect unlawful activity, or misconduct of a serious nature, that relates to the entity's functions or activities and giving access would be likely to prejudice the taking of appropriate action in relation to the matter; and
- giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body; giving access would reveal evaluative information generated within the entity in connection with a commercially sensitive decision-making process.

If the APP entity refuses to give access to the personal information or to give access in the manner requested by the individual, the entity must give the individual a written notice that sets out:

- the reasons for the refusal except to the extent that, having regard to the grounds for the refusal, it would be unreasonable to do so; and
- the mechanisms available to complain about the refusal; and
- any other matter prescribed by regulations made pursuant to the Act.

A sector specific access and correction framework applies in relation to credit related information.

If an APP entity holds personal information about an individual; and either the entity is satisfied that, having regard to a purpose for which the information is held, the information is inaccurate, out of date, incomplete, irrelevant or misleading; or the individual requests the entity to correct the information, the entity must take such steps as are reasonable in the circumstances to correct that information to

ensure that, having regard to the purpose for which it is held, the information is accurate, up to date, complete, relevant and not misleading (APP 13.1 (Correction)).

A breach of the APPs generally does not give rise to a cause of action exercisable at the suit of the affected individual. However, in certain circumstances the Commissioner can exercise jurisdiction and seek damages on behalf of an affected individual.

20 Cross-border disclosure and transfer of personal information

Transfer of PI is not regulated as such: the relevant act or practice that is regulated is use or disclosure of PI. Accordingly, it is not relevant whether the custody and control of the PI is transferred to the provider of outsourced processing services: it is sufficient if there is a disclosure, such as through the provider being provided with any form of access to the PI.

The transfer of PI to entities providing outsourced processing services in Australia, therefore, constitutes a disclosure of PI for the purposes of the Privacy Act. The Act makes no distinction between disclosure of PI to outsourced processing services and disclosure of PI to any other third party. Each disclosure would need to be undertaken subject to the requirements of APP 6 (Use and disclosure).

31304873_1 page | 25

APP 6 generally prohibits the disclosure of PI by organisations unless the disclosure is consistent with the primary purpose for collection of the information, or a related secondary purpose.

However, there is an exception under the Act in relation to use or disclosures by related bodies corporate: broadly, related bodies corporate are treated as a single entity for the purposes of privacy regulation.

APP 8 also imposes restrictions on the disclosure of personal information to recipients outside Australia: these restrictions apply in addition to the disclosure restrictions under APP 6.

As is the case with disclosures to third parties within Australia, transfer of PI to outside Australia is not regulated as such: for example, in relation to Australian regulated PI an organisation may transfer Australian regulated PI from its branch in Australia to another branch of itself outside Australia, or provide its overseas branch with electronic access to its Australian based database. However, any transfer to, or provision of electronic access (including read-only) to, Australian regulated PI to a third party 'overseas recipient', including a related body corporate of the discloser, is a disclosure of that PI. If the third party to whom the PI is disclosed is outside Australia, APP 8 (Cross-border disclosure) will operate.

APP 8 does not specifically address the common scenario of provision of custody and management of encrypted Australian regulated PI to a provider of outsourced hosting services. A sensible view is that unless there is any reasonable possibility that the provider of outsourced hosting services or persons that might reasonably be anticipated to have access to the PI might also have the capability to decrypt and thereby at least view personal information, there is no 'disclosure' of that PI to any overseas recipient. On this view, capability needs to be assessed 'in the round', having regard to technical capability of the provider of outsourced hosting services or persons that might reasonably be anticipated to have access to the encrypted PI), and operational and contractual safeguards against decryption or other misuse, taken together. OAIC's APP Guideline on APP 8 (Cross-border disclosure of personal information) at paragraph 8.14 suggests that the OAIC will consider the provision of personal information to cloud service providers located overseas for the limited purpose of storing and ensuring that the Australian regulated entity may access that information a 'use' rather than a 'disclosure' by the Australian regulated entity if:

- the contract with the provider requires the provider to only handle the information for these limited purposes;
- the contract with the provider requires that any sub-contractors to the provider must agree to the same obligations; and
- the contract gives the Australian entity effective control of how the personal information is handled by the overseas entity. According to the OAIC, contractual indicators that APP entity has retained effective control of the information include whether the entity has retained the right or power to access, change or retrieve the personal information, who else will be able to access the personal information and for what purposes, what types of security measures will be used for the storage and management of the personal information and whether the personal information can be retrieved or permanently deleted by the entity when no longer required at the end of the contract.

In practice, determining whether the provision of information to service providers constitutes a 'disclosure' or 'use' will likely be a difficult exercise and will ultimately turn on the nature of the services provided and the terms of the services agreement. APP entities are expected to take a cautious approach to this issue until further clarity around the concept of 'disclosure' is provided by the OAIC or the courts.

31304873_1 page | 26

APP 8 and section 16C of the Act also introduce an accountability approach to cross-border disclosures of personal information.

Before an organisation discloses personal information to an overseas recipient, the organisation must take reasonable steps to ensure that the overseas recipient does not breach the APPs (other than APP 1) in relation to that information. In some circumstances an act done, or a practice engaged in, by the overseas recipient that would breach the APPs, is taken to be a breach of the APPs by the organisation. Generally, this will apply where:

- APP 8.1 applies to the disclosure (APP 8.1 applies to all cross-border disclosures of personal information, unless an exception in APP 8.2 applies), and
- the overseas recipient is not subject to the APPs, but the act or practice would be a breach of the APPs if they were.

APP 8.2 lists a number of exceptions to APP 8.1. For example, APP 8.1 will not apply where:

- the organisation reasonably believes that the recipient is subject to a law or binding scheme that has the effect of protecting the information in a way that is, overall, substantially similar to the APPs; and there are mechanisms available to the individual to enforce that protection of the law or binding scheme (APP 8.2(a));

- an individual consents to the cross-border disclosure, after the organisation expressly informs them that APP 8.1 will no longer apply if they give their consent (APP 8.2(b)).

Each of these two exceptions is difficult to interpret and apply. Attempts to invoke the exceptions are likely to be the subject of significant debate and regulatory scrutiny.

As to the former, the OAIC has not issued a list of countries whose laws, or binding privacy schemes, that the OAIC considers have the effect of protecting the information in a way that is, overall, substantially similar to the APPs and allow for appropriately effective and available enforcement mechanisms. Law firms may be expected to be unwilling to 'sign off' based upon an 'overall' assessment of laws and remedies or as to a contractual scheme, noting the difficulties of such an assessment and the exposure of the Australian entity to strict liability under section 16C in the event of any subsequent determination by the OAIC (or court enforcing a determination of the OAIC) that the foreign laws or a scheme did not in fact not qualify for the exception in APP 8.2(a). However, the OAIC's Guidelines (at paragraph 8.21) do give some support to the use of binding corporate rules (BCRs) by international organisations, at least where the BCRs reflect "the stringent, intra-corporate global privacy policy that satisfies EU standards".

As to notice and consent, the form, prominence (conspicuousness) and level of comprehensibility of the 'express informing' are likely to be controversial. It is clear that the express notice needs to be sufficiently clear, but to ensure fully informed consent must the notice spell out what the practical effect of APP 8.1 not applying will be? The Commissioner's Guidelines (at paragraphs 8.28 to 8.30) are not prescriptive as to the form of notice, beyond stating that at the minimum the statement should explain that if the individual consents to the exposure and the overseas recipient handles the personal information in breach of the APPs, the (Australian regulated) entity will not be accountable under the Privacy Act and the individual will not be able to seek redress under the Privacy Act. Many notices as recently revised do not comply with these 'minimum' requirements. For example, consider a notice as follows (following a description of permitted purposes): You consent to your personal information being disclosed to a destination outside Australia for these purposes, including but not limited to the United States of America, and you acknowledge and agree that Australian Privacy Principle 8.1 will not apply to such disclosures and that we will not be required to take such steps as are reasonable in the circumstances to ensure such third parties outside of Australia comply with the Australian Privacy Principles. The notice does not include the second limb required by the Commissioner: it does not state that the individual will not be able to seek

redress under the Privacy Act. Other questions remain. How prominent does this notice need to be? If the consent is to have an ongoing operation, does the notice or consent need to be reinforced, or otherwise the subject of reminders, at periodic intervals, and if so, how often? Is the form of consent required for APP 8.2(b) different to the form of consent for other purposes, noting in this regard the unusual juxtaposition in the drafting of APP 8.2(b) of expressly informs and after being so informed, the individual consents?.

APP 8.2 also introduces a number of other circumstances in which APP 8.1 will not apply:

- where the cross border disclosure is required or authorised by or under an Australian law, or a court/tribunal order (APP 8.2(c));
- where an organisation reasonably believes that the disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety (APP 8.2(d), s16A item 1);
- where an organisation reasonably believes that the disclosure is necessary to take action in relation to the suspicion of unlawful activity or misconduct of a serious nature that relates to the organisation's functions or activities (APP 8.2(d), s 16A item 2);
- where an organisation reasonably believes that the disclosure is necessary to assist any APP entity, body or person to locate a person who has been reported as missing (APP 8.2(d), s 16A item 3).

The transfer of PI outside Australia does not require the transferor to notify, or seek the authorisation of, a supervisory authority.

The restrictions of APP 8 apply equally to overseas transfers to service providers as to other overseas recipients. The accountability requirements of APP 8 and section 16C of the Act apply in respect of the first recipient and any subsequent recipient.

However, an act or practice engaged in outside Australia does not breach the APPs if that act or practice is required by an applicable law of a foreign country.

21 Credit related provisions

Probably the most complex changes to the Privacy Act are the credit related provisions now completely redrafted in Part IIIA of the Privacy Act 1988 (Cth) (Privacy Act) (the CR Scheme).

The CR Scheme applies exclusively to the collection, use and disclosure of personal credit-related information about individuals and regulates the handling of a particular type of personal credit-related information, namely credit information. Credit information comprises, on the whole, information about an individual's consumer credit history. However, credit information may also include some information about an individual's commercial credit history. One example is court proceedings information about an individual, which may relates to both commercial and consumer credit history.

The CR Scheme sets out the limited purposes for which a credit provider may use an individual's credit information. These permitted purposes include the assessment of an application for consumer credit or commercial credit (the latter only with the individual's express consent). As such, the application of the CR Scheme is not necessarily dependant on whether an individual is applying for consumer or commercial credit. Rather, the determining factor as to the Scheme's application is whether a credit provider is proposing to collect, use or disclose credit information about an individual.

The majority of the restrictions in the CR Scheme address collection, use and disclosure of credit information in the course of a credit provider's engagement with a credit reporting bureau, such as Veda Advantage or Experian. (There are also other provisions that deal specifically with a credit provider's disclosure of information to other entities, such as debt collectors). Accordingly, if a credit provider does not collect from a CRB, or disclose to a CRB, credit information about individuals, many of the key provisions in the CR Scheme are not applicable.

The following categories of credit information are regulated under the Scheme.

- As noted above, the first and foundational category of information regulated by the CR Scheme

is called credit information. In basic terms, credit information is essentially the personal credit-related information a credit provider collects from its dealings with an individual and discloses to a CRB. Credit information is defined exhaustively in the CR Scheme to include limited kinds of personal credit-related information, such as identification information, default information and repayment history information.

- Credit information is repackaged and consolidated with other information held by a CRB to form credit reporting information. Credit reporting information includes credit information and any information derived by CRB from the credit information. CRBs disclose credit reporting information about individuals to credit providers that request the information.

- In the hands of a credit provider, credit reporting information becomes credit eligibility information, which comprises the credit reporting information that is obtained from a CRB and any other information a credit provider derives from that information. The restrictions in the CR Scheme that govern use and disclosure of credit eligibility information by a credit provider apply only to information obtained from a CRB (and information derived therefrom) and not any other information a credit provider may have collected directly from the individual.

The CR Scheme must be read in conjunction with the terms of the Credit Reporting Privacy Code (CR Code). The CR Code is legally binding on credit providers and sets out further and more detailed restrictions and obligations relating to (among other things) the collection, use and disclosure of personal credit-related information.

For the purpose of determining whether an organisation is a credit provider under the CR Scheme in relation to a particular transaction, it is irrelevant whether Bauer provides a customer with consumer credit or commercial credit. This distinction only becomes relevant in relation to the purposes for which the entity may use and disclose credit information. Section 6G of the Privacy Act describes a number of scenarios in which an entity is deemed to be a credit provider. Of most general relevance, an organisation is a credit provider if it carries on a business in the course of which it provides credit in connection with the sale of goods, or the supply of services, by the supplier; and the credit is available for at least 7 days.

22 Emerging trends and issues

Emerging trends in Australian privacy law will reflect global trends, concerns and issues as they arise. Australia tends to closely follow major global trends, paying particular attention to regulatory developments in the U.S.A., European Union and ASEAN region.

Current trends include:

- Applications for registration and registrations of APP codes. The amendments to the Act effective from March 2014 give a prominent role to enforceable industry Codes. It is expected that there will be significant industry sector activity in development of Codes.

- Possible introduction of mandatory data breach notification requirements.

- Increased focus upon privacy by design and information security by design principles and practical implementation of privacy protective processes and systems by corporations.

- Review of published privacy policies for 'transparency': prominence, readability and structuring appropriate to the likely readers and as to the description of primary and secondary purposes of personal information.

- Pressure for expansion of privacy protection in relation to surveillance and geo-tracking devices and extension of the definition of personal information, or introduction of new restrictions as to ‘profiling’, to address concerns as to particular, perceived socially detrimental uses of big data analytics.

- Extension of privacy policy development and privacy and information security related enforcement activities by the Australian Communications and Media Authority (www.acma.gov.au), a well-resourced regulator by comparison with the OAIC.

- Changes to privacy regulation of news gathering and news reporting by the print and electronic media. It is likely that media Codes or other media regulation affecting privacy will change in the foreseeable future.

- The ALRC’s consultation and report (due June 2014) as to introduction of a statutory cause of action for serious invasion of privacy.

- Continuing pressure for more extensive regulation of third party online behavioural advertising. As at January 2014 there had not been an active ‘do not track’ debate in Australia.

- More active cross-border coordination and joint enforcement activity by the OAIC and comparable regulators in other jurisdictions.

- Continuing consultation as to alignment of privacy regulation in the Asia Pacific region.

Focus upon law enforcement exceptions to privacy laws following the Edward Snowden revelations as to activities of the U.S. National Security Agency and national security collaboration between the ‘Five Eyes’ countries, including Australia.

Given the volatility and unpredictability of emergence of issues in privacy regulation, it is likely that the above list will change by addition of further issues.

11 March 2014

Peter Leonard
Partner, Gilbert + Tobin Lawyers
T +61 2 9263 4003
pleonard@gtlaw.com.au

EPIC --- Privacy and Human Rights Report 2006

http://www.worldlii.org/int/journals/EPICPrivHR/2006/PHR2006-Australi.html December 08, 2014

EPIC --- Privacy and Human Rights Report: ... The third and latest attempt at a comprehensive review of the Privacy Act by the Australian Law Reform Commission ...

While privacy issues are now featured prominently in the daily news in Australia, the legal safeguards for personal information remain limited. Neither the Australian Federal Constitution nor the Constitutions of the six States and two Territories contain any express provisions relating to privacy.

However, in 2004 the Australian Capital Territory (ACT) became the first jurisdiction to incorporate a bill of rights. Section 12 of the Human Rights Act 2004 (ACT) creates a right of "privacy and reputation."[1081] The Human Rights Act incorporates international human rights standards into local ACT law by requiring all ACT laws to be interpreted consistently with human rights "as far as possible." The ACT Human Rights and Discrimination Commissioner has functions including reviewing the effect of ACT laws on human rights, reporting to the Attorney General. The Commissioner's reports must later be tabled in the Legislative Assembly. However, the Commissioner does not have power to handle complaints.

The State of Victoria adopted a similar approach in 2006, with the public sector bound beginning January 2008 to observe a variety of civil and political rights, including the right to privacy, when they create laws, set policies and provide services. All new laws will require a Statement of Compatibility to tell Parliament whether they meet human rights standards. In exceptional circumstances Parliament may strike down a law that does not uphold human rights.[1082]

The Australian Constitution limits the legislative power of the Australian (federal) government, with areas not expressly authorized being reserved for the States.[1083] The constitutionality of federal laws imposing privacy rules on the private sector has been questioned, but not so far challenged. Most commentators believe that the federal government could base any private sector privacy law on a "cocktail" of constitutional powers including those giving authority over telecommunications, corporations and foreign affairs (e.g., treaties).

Privacy Law in Australia comprises several federal statutes covering particular sectors and activities, some State or Territory laws with limited effect, and the residual common law protections.

In Australia there has until recently been no recognition of a general tort of protection of privacy. Very occasionally the common law been used in support of privacy rights through actions for breach of confidence, defamation, trespass or nuisance. The New South Wales Law Reform Commission was asked in 2006 to examine the desirability of developing a statutory tort of privacy.[1084] It is expected to report in 2008.

An affirmation of this common law right was issued in a 2007 Victorian County Court case, in which the ABC media organization was ordered to pay a rape victim AUD 234,190 (149,000 EUR) in damages after she was named on air.[1085] The damages were awarded for breach of privacy and breach of confidence caused by the unjustified publication, and related to post-traumatic stress, loss of earnings and medical expenses, as well as for hurt and distress, embarrassment, humiliation and shame. The ABC has announced it will appeal the ruling on the basis that no such tort of privacy exists in Australian law.[1086]

The principal federal statute is the Privacy Act of 1988,[1087] which has four main areas of application and which gives partial effect to Australia's commitment to the Organization for Economic Cooperation and Development (OECD) Guidelines and to the International Covenant on Civil and Political Rights (ICCPR), Article 17. It creates a set of 11 Information Privacy Principles (IPPs), based on those in the OECD Guidelines that apply to the activities of most federal government agencies. A separate set of rules about the handling of consumer credit information, added to the law in 1989, applies to all private and public sector organizations. The third area of coverage is the use of the government issued Tax File Number (TFN), where the entire community is subject to Guidelines issued by the Privacy Commissioner, which take effect as subordinate legislation. The fourth area of coverage, which only commenced in December 2001, is widespread private sector organizations regulated by the National Privacy Principles (NPPs). However, private companies can apply to the Privacy Commissioner for approval of a self-developed Code of Practice containing principles that are an "overall equivalent" to the NPPs. In addition, the Act provides for several broad exemptions for employee records; media organizations; political parties; and small businesses.

According to the Federal Government the small business exemption will exempt about 94 percent of all Australian businesses but only 30 percent of total business sales, an exception that includes many Internet companies.[1088] The breadth of the exemption for political parties was demonstrated in March 2005 when the Privacy Commissioner had to decline a request to investigate complaints regarding telemarketing activities during the campaign period for the October 2004 federal election, including the use of spam,[1089] and allegations that the Liberal Party had accessed silent telephone numbers to make political canvassing calls.[1090] The exemption also excludes from view the increasing use of databases by political parties to track voter preferences and create customized marketing material for voters.[1091]

There are also weaknesses in the enforcement regime including, for example, allowing privacy complaints to be handled initially by an industry-appointed code authority, although a right of appeal to the Privacy Commissioner was inserted by Opposition parties. The Act does, however, include an innovative principle of anonymity. However, the mere existence of the anonymity principle has not prevented the development of electronic road tolling systems that identify every vehicle, and the impact of this principle on the development of electronic health records, for example, remains to be seen.

The Privacy Act of 1988 has been widely criticized as failing to meet international standards of privacy protection. The 2004 amendments to the Privacy Act included extending correction rights to non-Australians, extending the scope of the transborder data flow control (Principle 9) to data about non-Australians, and ensuring that the Privacy Commissioner could approve Codes of Practice that voluntarily covered otherwise exempt acts and practices.[1092] The third and latest attempt at a comprehensive review of the Privacy Act by the Australian Law Reform Commission (ALRC) is not due to report its findings until 2008.[1093]

There are two other federal privacy-related laws for which the federal Privacy Commissioner is also the supervisory and complaint handling agency. The first one is Part VIIC of the Crimes Act,[1094] enacted in 1989, which provides some protection to individuals who have had criminal convictions in relation to so-called "spent" convictions (i.e., convictions for relatively minor offenses which they are allowed to "deny" or have discounted after a set period of time). The second one is the Data-Matching Program (Assistance and Tax) Act 1990[1095] that provides detailed procedural controls over the operation of a major program of information matching between federal tax and benefit agencies.

The Office of the Federal Privacy Commissioner enforces the Privacy Act.[1096] The Office has wide range of functions, including handling complaints, auditing compliance, promoting community awareness, and advising the government and others on privacy matters. The Commissioner has so far approved three Codes of Practice under the private sector regime: for the General Insurance Industry, which has its own adjudicator for complaints, the Licensed Clubs in the state of Queensland, which defaults to the Privacy Commissioner for complaints, and the "Market and Social Research and Privacy Code" for the Association of Market Research Organisations.[1097] The Code provides some standards that are higher than the NPPs, including giving the data subject the right to choose whether to destroy or de-identify their information after use.[1098]

As of 2006, the Office had 40 full-time staff and seven part-time staff divided into four sections: Compliance, Policy, Corporate and Public Affairs, and the Executive.[1099] The number of complaints received in the period from July 2005 to June 2006 totaled 1,183, slightly less than the previous year. 62% of the complaints concerned application of the NPPs to the private sector; 14% concerned credit reporting; and 13% concerned the information privacy principles.[1100] The largest categories of complaints concerned the financial industry (202); followed by the Australian Government (159); the debt/credit industry (131); health service providers (123); telecommunications and Internet service providers (83); landlords and real estate agents (59); insurance organizations (41); and retail (31).[1101] In 2005-06 the Commissioner's office also received 19,150 telephone enquiries. [1102]

Section 52 of the Privacy Act provides that the Commissioner may make formal determinations in relation to complaints investigated. The determination by the Commissioner may dismiss the complaint, or may find the complaint substantiated and declare that the respondent should cease to breach the Act, take any reasonable steps to redress damage suffered by the complainant, or pay compensation to the complainant. Importantly, Section 52 determinations are not legally binding on the respondent. The Commissioner, the complainant, or the adjudicator for an approved privacy code can commence proceedings in the Federal Court or Federal Magistrates Court for an order to enforce a determination.

In a rash of self-reporting of privacy breaches in mid-2006, Federal Government agencies Centrelink (the social security benefits agency), the Child Support Agency and the Australian Taxation Office each admitted they had found multiple cases of staff inappropriately accessing, amending, using and disclosing customer records. Centrelink found 600 staff over a two-year period had committed 790 breaches; of these, 19 were sacked and almost 100 resigned. The Child Support Agency discovered 405 breaches, including 69 cases where sensitive information including addresses was given to former spouses. At the Taxation Office, 16 of 27 offending staff were sacked or resigned.[1103]

The Victorian State Police have also been subject to a series of embarrassing privacy breaches. In 2005 the Office of Police Integrity called for the Police's LEAP database to be scrapped because of a series of security breaches. The Office of Police Integrity itself later mistakenly posted LEAP files on more than 400 people to a single complainant, and an IBM technician authorised to audit the LEAP system accidentally emailed files on up to 1,000 people to a whistleblower. Another case saw details of a person's criminal record wrongly attributed to another person after a routine records check for an employer.[1104]

A complex mix of privacy standards applies to the telecommunications sector. The Telecommunications Act 1997[1105] contains a detailed list of exceptions from a basic presumption of confidentiality of customer records.[1106] These exceptions are similar to those in the Use and Disclosure Principles of the federal Privacy Act. An Industry Forum prepares detailed codes and guidelines, some of which are binding.[1107] A Code of Practice on the Protection of Customer Personal Information that was binding on all telecommunications carriers and service providers was de-registered once the private sector amendments to the federal Privacy Act took effect. The enforcement position remains confusing, with the Australian Communications and Media Authority (ACMA); the Telecommunications Industry Ombudsman and the Privacy Commissioner all having overlapping jurisdictions. There is also a binding Code of Practice on Calling Number Display (CND),[1108] which requires carriers to offer free per call and per line blocking (but only on an opt-out basis) and attempts to impose guidelines on telephone users' use of CND information. Other Codes deal incidentally with privacy issues such as directories, numbering and emergency calls.

Complaints were made in 2003 to both the ACA (as the ACMA was then known) and the Privacy Commissioner about the use by ISPs of "blocked" CND information (including on silent lines).[1109] The ACA investigation found unlawful conduct, but declined to take action. Findings by the Privacy Commissioner, and by the Ombudsman in relation to the ACA's failure to act, are awaited. The ACMA has also investigated the use of telephone directory data and in May 2005 issued a draft Standard, with a further revised draft issued in April 2006.[1110]

The Telecommunications (Interception) Act of 1979[1111] regulates the interception of telecommunications. A warrant is required under the Act and it also provides for detailed monitoring and reporting. However, the Interception Act safeguards need to be read alongside Part 15 of the Telecommunications Act 1997 that places obligations on telecommunications providers to provide an interception capability and positively assist law enforcement agencies in relation to interception. There have been several changes to the interception regime in recent years, including broadening the range of offenses for which warrants can be obtained; allowing more law enforcement agencies to apply for warrants and more of them to execute warrants themselves; and transferring the warrant issuing authority from federal court judges to designated members of the Administrative Appeals Tribunal (who are on term appointments rather than tenured and are arguably less independent). Significant loopholes exist within the legislation, and uncertainty in relation to allowable "participant monitoring."[1112]

Telecommunications interception activity continues at a high level. In 2005-06, the number of warrants issued for telecommunications intercepts was 2,934, of which only 5 were withdrawn or refused.[1113] Statistics are not yet available on the numbers of warrants issued to access emails and text messages, under new stored communications warrant powers passed by Parliament in March 2006.[1114] The new powers extend to all the communications of 'innocent' people, known as B-parties, who have communicated with someone suspected of a crime. The Government does not need to tell B-parties that their communications have been monitored.[1115]

Additional federal legislation has further weakened surveillance protections. The Surveillance Devices Act 2004 increased the number of offenses for which surveillance may be initiated by law enforcement and anti-corruption agencies (both Federal Government and State/Territory agencies), and broadened the justifications beyond criminal matters to also include child recovery.[1116] The types of surveillance available are data surveillance, listening devices, optical surveillance and tracking devices. Warrants may be issued by a judge, a member of the Administrative Appeals Panel, or even, in exceptional circumstances, by a senior public servant.

The first annual report on the operations of the Surveillance Devices Act, produced by the Attorney-General's Department, noted that in the six and a half months of operation to July 2005, 235 warrants were issued to the Australian Federal Police, and a further 22 to the Australian Crime Commission. No applications for warrants were refused.[1117] A further 33 tracking device authorisations were made within those two agencies, without seeking a warrant; again, no requests were refused. The warrants and authorisations led to 73 arrests and 71 prosecutions, but only 5 convictions during the reporting year.

The Crimes Act[1118] also contains a range of other privacy related measures, such as offenses relating to unauthorized access to computers, unauthorized interception of mail and telecommunications and the unauthorized disclosure of Commonwealth government information.[1119]

In September 2003, an online censorship bill was passed, allowing the Australian Broadcasting Authority and the Office of Film and Classic Literature to withhold information regarding what online information is being restricted.[1120] The amendments to the Freedom of Information (FOI) Act prevent public scrutiny (and potential criticism) of the operation of the Federal Internet censorship regime that became operative on January 1, 2000. The Act restricts the details regarding the net blocking system that restricts access to material that is "objectionable" or "unsuitable for minors."[1121] Under Australia's FOI law, the agencies may withhold information regarding their practices and the details of their agency operations. Earlier in 2003, Electronic Frontier Australia (EFA) and other civil liberties groups had opposed the Internet content regime put in place under the Broadcasting Services Act, and had tracked the operation of the laws through FOI applications.[1122]

Spam legislation (Spam Act 2003) became effective April 2004, outlawing unsolicited marketing messages on electronic mediums including email, SMS (short message service), MMS (multimedia messaging service), and instant messaging; requiring opt-out facilities and an accurate sender address.[1123] Penalties range up to AUD 1.1 million (~USD 832,000) for businesses that repeatedly violate the law. Emailers must have prior consent of the recipient, although consent can be inferred from prior conduct and relationships.[1124] The Australian Communications and Media Authority will enforce the law, which has begun establishing enforcement capabilities, although early goals target compliance rather than prosecution.[1125] Civil liberties organizations have criticized the Spam Act because the search and seizure provisions allow some government employees and police to seize an individual's computer without a search warrant.[1126]

The first infringement notice issued under the Spam Act resulted in a car sales company paying a AUD 6,600 (~USD 5,000) fine for unwanted SMS text messages that were sent to the mobile telephones of people who had listed their numbers in classified advertisements to sell their cars.[1127] In the first two years of operation of the Spam Act, ACMA issued formal warning letters to 10 companies, entered into enforceable undertakings with five companies, issued 13 infringement notices, and launched its first major prosecution.[1128] ACMA claims that since the introduction of the Spam Act, spam received in Australia has fallen by 50%.[1129]

In October 2006 ACMA won a landmark prosecution against Clarity1 Pty Ltd, which was alleged to have sent out at least 231 million commercial emails in the first twelve months after the Spam Act commenced, with most of these messages unsolicited and in breach of the Act. The company was ordered to pay AUD $4.5 million, and the company's director was ordered to pay a further AUD $1 million.[1130]

In May 2007 a Do Not Call register was launched, with 50,000 registrants in the first few hours alone. Unlike similar schemes in the UK and USA, telemarketing firms in Australia will, from June 2007, need to provide their databases to the register, and the register operators will 'wash' the databases for them – for a fee.[1131] Companies contacting people who have listed themselves on the register face fines of up to AUD $1.1 million. However, exempt groups, which include charities, political parties, social researchers and educational institutions, are said to account for 80% of the 800 million telemarketing calls made each year.[1132]

The National E-Health Transition Authority (NeHTA) was created in July 2005 to develop national health information management and information and communication technology standards and specifications. NeHTA is jointly funded by the States, Territories and Australian Governments, and its governance ensures equal participation by all jurisdictions.[1133]

NeHTA is working on a number of initiatives, many of which are the necessary first steps towards a national electronic health records system – things like ensuring different IT systems are interoperable, that there is a system for identifying patients and clinicians accurately and uniquely, and that everyone uses the same 'language' when describing medical conditions and medicines. One of NeHTA's projects is to develop a national model of E-Health Consent for the States and Territories to follow when implementing their systems. That model has not yet been finalised. A key question will be whether the model will follow an "opt in" or an "opt out" model of consent.

Meanwhile the New South Wales State Government has been working on its own electronic health records project, Healthelink.[1134] Despite the NSW health privacy law requiring express consent before a patient is placed on a system to link electronic health records across organizations, it was revealed in June 2005 that pilots planned for late 2005 were being developed instead on the basis of a compulsory record, with only an "opt out" choice as to the sharing of the record with other health service providers.[1135] The Government exempted itself from the "express consent" requirement by way of regulation, and began the pilots in 2006. Participation by General Practitioners has been low because of their privacy concerns about the system's design.[1136]

An emerging health privacy issue is the use of software in General Practitioners' offices, which automatically extract patient data, for sale to pharmaceuticals companies. The Federal Privacy Commissioner dismissed a complaint because the patient data was being de-identified.[1137] However, the political reaction to the Commissioner's decision was strong enough that she made a clarifying media statement.[1138] The federal Minister for Health, the Opposition's Shadow Minister, and minor parties, all criticized the practice based on the risk of de-identification.[1139]

A major report on genetic privacy was issued in March 2003 by the Australian Law Reform Commission and the Australian Health Ethics Committee of the National Health and Medical Research Council. "Essentially Yours" makes 144 recommendations about the ethical, legal and social implications of genetic privacy.[1140] The report recommends that privacy laws be harmonized and tailored to address the particular challenges of human genetic information, including extending protection to genetic samples, and acknowledging the familial dimension of genetic information. Employers should not be permitted to collect or use genetic information – except in those rare circumstances where this is necessary to protect the health and safety of workers or third parties, and the action complies with stringent standards set by a new Human Genetics Commission of Australia (HGCA). The insurance industry should be required to adopt a range of improved consumer protection policies and practices with respect to its use of genetic information (including family history) for underwriting purposes. A new criminal offense should be created to prohibit someone submitting another person's sample for genetic testing knowing that this is done without consent or other lawful authority. DNA parentage testing should be conducted only with the consent of each person sampled (or both parents in the case of young children), or pursuant to a court order.

The Australian Government is preparing a response to the "Essentially Yours" report, although a number of recommendations have already been acted on.[1141]

A new legislative framework for widespread financial surveillance and secret reporting has recently been put in place. The proposed Anti-Money Laundering and Counter-Terrorism Financing Act 2006 imposes a number of obligations on businesses when they provide certain services, including customer due diligence (identification, verification of identity and ongoing monitoring of transactions), reporting (suspicious matters, threshold transactions and international funds transfer instructions), and record keeping. The Act is due to commence in December 2007.

The first series of reforms covers the financial sector (including banks, credit unions and building societies), as well as gaming services (casinos, clubs and wagering service providers) and bullion dealers. The second series of reforms will cover real estate agents, dealers in precious metals and dealers in precious stones and a range of non-financial transaction provided by accountants, lawyers and trust and company service providers.[1142]

In 2001 the Prime Minister announced the establishment of a national digital database of DNA and fingerprint samples in order to facilitate law enforcement.[1143] CrimTrac, a Commonwealth agency, coordinates the national DNA database system. The system when fully operational will enable the comparison of DNA profiles across all Australia's jurisdictions for law enforcement purposes. Commonwealth, State and Territory legislation underpin the system. A Report of a Review of Part 1D of the Crimes Act 1914 (the relevant federal law) was tabled in Parliament on 15 May 2003. The Review found that the national system is not yet operational and only one jurisdiction (New South Wales) has loaded profiles onto the relevant CrimTrac database known as the National Criminal Investigation DNA Database (NCIDD).

While there has been relatively little experience of the operation of Part 1D, the Review has recommended improved accountability arrangements both within and across Australia's jurisdictions. The Review sees effective accountability mechanisms as crucial to maintaining public confidence in the use of DNA analysis for law enforcement purposes. The Review recommends that the external scrutiny mechanisms be based upon existing cooperation between Australian Ombudsmen with involvement of Privacy Commissioners and other monitoring bodies. Under legislation proposed by the Victoria Law Reform Committee, suspected thieves would be required – if compelled by police via a court order – to submit DNA samples.[1144] Currently only suspects of more serious crimes, such as rape and murder, can be required to submit DNA.[1145]

Legislative amendments in 2002 and 2003 have given the Australian Security Intelligence Organization (ASIO) significant and highly controversial new powers, including the ability to detain and question individuals suspected of having information relevant to terrorism. Despite extracting many concessions and additional safeguards from the government, the Opposition allowed the final changes through in June 2003 without ruling out the possibility of indefinite detention without charges under repeated warrants. The amendments allow ASIO to detain and question a journalist who may have information regarding suspected terrorists gained through her interviews and contacts; refusing to cooperate could result in a five-year imprisonment.[1146] While the amendments included a sunset clause, which lapsed in July 2006, the laws have been renewed. The budget for ASIO has doubled since September 11, 2001, after receiving an AUS 131 million boost in 2004.[1147]

In November 2003, Australia introduced the "M-Series" tamper resistant passports.[1148] In order to meet the requirements of the United States Visa Waiver Program, the Australian government fast-tracked legislation amending the Australian Passports Act in order to provide facial biometric features in passports.[1149] A Passports Legislation Consultation Group was established, including members from privacy and human rights groups as well as travel, financial and biometrics industries.[1150]

The federal Department of Foreign Affairs and Trade began issuing biometric e-passports, incorporating an unencrypted RFID chip in October 2005, to meet the demands of the US.[1151] Privacy advocates warned of the dangers of "skimming" and "eavesdropping."[1152] The Department finally acknowledged these concerns and changes were made to the e-passport's design.[1153]

The Australian Government, in conjunction with the States and Territories, developed a National Identity Security Strategy in 2005. The projects under way under the auspices of this strategy include the development of a common range of proof of identity documents which government agencies will be able to use to identify clients who register with them for services, the identification of appropriate security standards on those key proof of identity documents, the identification of key data matching elements to improve the integrity of identity information held on existing government databases; and authentication of individuals accessing services.

A further project being developed under the National Identity Security Strategy is the Document Verification Service (DVS). The DVS has been described as an online service to check the validity of proof of identity documents against the issuing agency. The DVS project is therefore about flushing out fake foundation documents, such as a fake driver's license or birth certificate, which is then used to apply for a passport or for social security benefits.[1154]

The Australian Government announced in the 2006–07 Budget that the DVS will be rolled out with funding of $28.3 million, building on a prototype service trialed during 2006. The DVS is intended to be a secure, electronic, online system accessible by all key Australian Government, State and Territory agencies, and potentially by the private sector. Agencies authorized to use the DVS will be able to check in real time whether a document presented to them as a proof-of-identity by an individual applying for high value benefits and services was issued by the relevant agency, and that the details on the document are true and accurate. [1155]

Very little information about the DVS is available publicly, and no independent Privacy Impact Assessment has been done. Any internal privacy impact assessment, or evaluation of the pilot (if either has even been done), has not been published.[1156] Amendments to electoral laws commencing in April 2007 will require new forms of 'proof of identity' for people wishing to enroll to vote, re-enroll, or change their address or other details.[1157]

In April 2005, the NSW Government introduced a new law, to allow the motor vehicle and driver-licensing agency, the Roads and Traffic Authority, to start issuing photographic identity cards to non-drivers. The Photo Card Act 2005 allows the Authority to hold personal information about non-drivers on the same database as for all drivers in the State, and to issue cards using the same unique numbering system.[1158] The Australian Privacy Foundation campaigned against the proposal, seeing it as introducing a State-based universal identity card by stealth.[1159]

The Australian Government announced in April 2006 that it would introduce a new 'Access Card' in 2008. The Access Card is intended to replace a number of existing cards, including the universal Medicare health benefits card, and various social security benefit cards issued by Centrelink and the Department of Veterans' Affairs. The card would be compulsory from 2010 for anyone who wished to access any of his or her health or social security entitlements.[1160]

The Government proposes to use smart card technology to hold large amounts of data on a chip inside the card. In addition, some information would be clearly visible on the face and back of the card, including the cardholder's name, photograph, signature and card number.

The Access Card would be supported by a new centralised, national population database, the Access Card Register. The database would hold details of children as well as adults, but only adults would be issued with a card (with some exceptions). The database would include biometric photographs, with the intended purpose being facial recognition for a variety of benefits administration, immigration and general law enforcement purposes. Registration for the card is intended to begin in 2008, and will require adults to attend a government office, prove their identity, and be photographed.

A wide variety of groups has criticized the proposal as a de facto national ID card.[1161] In March 2007 the authorizing legislation was withdrawn from the Senate by the Government, following unanimous criticism from a multi-party Senate Committee.[1162] The Government has announced its intention to re-introduce legislation in June 2007.

The federal Freedom of Information Act of 1982 provides for access to government records, requiring agencies to respond within 30 days to requests. The FOI Act is the mechanism through which the access right in the Privacy Act is implemented for public sector agencies. The Commonwealth Ombudsman promotes the FOI Act and handles complaints about procedural failures. Merits review (appeal) of adverse FOI decisions is provided by the Administrative Appeals Tribunal, with the possibility of further appeals on points of law to the Federal Court. Budget cuts have severely restricted the capacity of the Attorney General Department and Ombudsman to support the Act and there is now little central direction, guidance or monitoring. In 2002-2003, there were 41,481 requests, an 11 percent increase over the previous year; of those finalized, 71 percent were granted in full, 23 percent granted in part, and 6 percent refused. Nearly 92 percent of the requests were for personal information, mostly to the Department of Veterans' Affairs, the Department of Immigration and Multicultural and Indigenous Affairs (DIMIA), and Centrelink (a government agency delivering a range of Commonwealth services). In 2001, the Senate held an inquiry into whether to adopt changes recommended by a 1995 report critical of the FOI law, but no substantive changes have since been made to the law.

The Australian States and Territories have varying privacy laws. New South Wales (NSW), the most populous State, passed the Privacy and Personal Information Protection Act 1998 (PPIP Act) which applies (since July 2000) to most state government agencies and all local councils, although there are numerous and generous exemptions, and agencies can apply for temporary directions, regulations or Codes of Practice that can weaken the principles.

The PPIP Act is based on a set of OECD-style Information Protection Principles and requires all government departments and agencies to develop a Privacy Management Plan demonstrating their compliance plans. It also allows for the development of Codes of Practice that weaken the Information Protection Principles, and several such Codes have already been made.[1168]

The NSW Attorney General's Department in 2004 conducted a statutory five-year review of the PPIP Act, but its results have not been released. [1169] The NSW Privacy Commissioner commented on the legislation in a comprehensive submission in June 2004.[1170] The New South Wales Law Reform Commission has since been asked to review the Act, and is due to report in 2008.[1171]

In 2002, a new health-specific law, Health Records and Information Privacy Act 2002 (HRIP Act), took health information out of the scope of the PPIP Act. Instead, health information is regulated by 15 Health Privacy Principles, which apply to the private sector as well as State and local government agencies.[1172] The HRIP Act commenced on September 1, 2004.

NSW enacted a Workplace Video Surveillance Act[1173] in 1998 (partly in response to a Privacy Committee report). This was replaced in 2005 with the broader Workplace Surveillance Act 2005, which covers camera surveillance, email and internet monitoring and location tracking in the workplace. The Australian Privacy Foundation has criticized the Act as weak in its level of actual privacy protection, and difficult in terms of implementation for employers.[1174]

In an interim report issued publicly in early 2002,[1175] the NSW Law Reform Commission reviewed the laws governing surveillance more generally, including the operation of the existing Listening Devices Act 1984.[1176] The Law Reform Commission completed its review and reported to the Attorney General in May 2005, but after two years the Attorney General has still not yet approved the report for publication.[1177]

In July 2002, the Office of Information Technology (OIT), an agency of the state government of NSW, issued guidelines pursuant to the Privacy and Personal Information Protection Act of 1998. The guideline states that as a matter of good practice, each agency should have a designated privacy contact officer. It adds that the obligations of the chief information officer in each agency include ensuring there is a privacy management plan. The responsibilities of other staff, including librarians, web managers, human resources managers and records managers, are also described.[1178]

The State of Victoria has enacted the Information Privacy Act 2000, which applies privacy principles (an almost exact copy of the NPPs in the federal Act) to most state government agencies and local councils. There are relatively few exemptions and while there is provision for Codes of Practice, they cannot weaken the principles. The Act created an office of Privacy Commissioner,[1179] very active so far, with a monitoring, enforcement and education role, and to conciliate complaints.

The Victorian Civil and Administrative Tribunal can determine unresolved complaints. Victoria has also passed the Health Records Act 2001 to complement the information privacy legislation by requiring Victorian health service providers to handle health information responsibly. The Health

Records Act also gives patients a right of access to their records held by private practitioners. The Victorian Law Reform Commission[1180] received a reference in April 2001 to review the coverage of privacy law in Victoria. It published its final report on workplace privacy in October 2005, and is now turning its attention to surveillance in public places.[1181]

The government of the Australian Capital Territory (ACT), which used to be a local authority under Commonwealth (federal) law, and was consequently covered by the federal Privacy Act, achieved self-government as a separate Territory in 1989. The Privacy Act was amended to continue coverage, intended as an interim measure, but this remains the position, with the Federal Privacy Commissioner in effect serving also as the ACT's Commissioner, responsible to its own government. However, in 1997 the ACT government passed its own Health Records (Access and Privacy) Act,[1182] which applies to personal health information held by anyone in the public or private sector. Its provisions are similar to those of the IPPs in the Privacy Act, and supersedes them for ACT government agencies in this area of data handling.

The self-governing Northern Territory has enacted a combined privacy and FOI law – the Information Act 2002,[1183] which took effect in July 2003. The Office of the Information Commissioner was established in 2004.[1184]

Queensland had a purely advisory Privacy Committee from 1984 to 1991[1185] and has a limited privacy statute[1186] covering the use of listening devices, credit reporting (operating alongside the 1989 amendments to the federal Privacy Act) and physical intrusions into private property. In April 1998, after a yearlong review, a Parliamentary Committee recommended comprehensive privacy legislation for the public sector.[1187] The government indicated that it intended to legislate but no timetable has been set, and in 2001 the government adopted privacy principles on a hopefully interim non-statutory basis.[1188]

In Tasmania, the Personal Information Protection Act 2004 came into effect in September 2005.[1189] The Act covers state government and local councils in Tasmania. It does not establish a position of Privacy Commissioner, but gives complaint-handling responsibilities to the Tasmanian Ombudsman. The Minister can make public interest determinations allowing organizations to be exempt from any or all provisions of the Act. The Act covers health information and applies to deceased persons for 25 years after death.

The other states, South Australia and Western Australia, also operate administrative schemes based on variations of the standard sets of privacy principles.[1190] In May 2003, the Western Australian government released a discussion paper[1191] proposing a public sector privacy law.

All of the States and Territories also have FOI laws that include rights for individuals to access and correct personal information about themselves.[1192]

[1081] Section 12 states: Everyone has the right - (a) not to have his or her privacy, family, home or correspondence interfered with unlawfully or arbitrarily; and (b) not to have his or her reputation unlawfully attacked. See <http://www.austlii.edu.au/au/legis/act/consol_act/hra2004148/>.

Canberra to move on privacy law

http://www.theage.com.au/national/canberra-to-move-on-privacy-law-20110720-1hp19.html December 08, 2014

Australians could secure new rights to defend their privacy in the wake of the phone hacking scandal that has engulfed Rupert Murdoch's media empire.

AUSTRALIANS could secure new rights to defend their privacy in the wake of the phone hacking scandal that has engulfed Rupert Murdoch's media empire.

The Gillard government will today move towards new laws that would allow Australians to sue for damages in the event of a serious invasion of their privacy.

Ahead of today's announcement, federal Privacy Minister Brendan O'Connor told The Age the government was ''very serious about having this discussion'' following the UK scandal. He said he was confident any change would preserve reasonable media freedom. ''There are two ideals we uphold as a government - freedom of speech, and people's right to have a private life,'' Mr O'Connor said.

The launch of a consultation period for privacy reform is a pre-emptive strike by the government, given the Greens have called for a wider inquiry

to examine the concentration of media ownership and privacy issues.

Mr O'Connor said the government would shortly release a discussion paper flagging a statutory right to sue for ''serious'' privacy invasions, rather than letting the system of privacy regulation evolve in an ad hoc way through court decisions.

Media companies, including News Ltd and Fairfax Media, owner of The Age, have previously opposed significant privacy reform, given its potential to limit freedom of speech.

Fairfax Media general counsel Gail Hambly said the company had historically opposed a separate statutory right to sue for privacy given Australia's lack of constitutional protection for free speech. ''However, if there is a consultation process, we'll be keen to participate,'' she said.

The ABC also said it would like to be part of any public debate.

The looming privacy debate comes as Prime Minister Julia Gillard yesterday provoked News Ltd - the Australian arm of Mr Murdoch's media empire - by declaring the company would face ''hard questions'' in the wake of the UK scandal.

''When people have seen telephones hacked into, when people have seen individuals grieving have to deal with all of this, then I do think that causes them to ask some questions here in our country, some questions about News Ltd here,'' she said.

''Obviously, News Ltd has got a responsibility to answer those questions when they're asked.''

Government sources suggested Ms Gillard had not intended such a sharp rebuke to Rupert Murdoch's Australian operation, which includes The Australian and Herald Sun.

But her intervention only hours after Rupert and James Murdoch were grilled by a British parliamentary committee generated international headlines and further escalated tensions between Labor and News.

A senior News Ltd executive called prime ministerial staff in an attempt to clarify what Ms Gillard meant, but according to company sources, received no response.

News Ltd chairman John Hartigan issued a stinging rebuke, declaring in a statement: ''The Prime Minister's comments seek to draw a link between News Corporation operations in the UK and those here in Australia. The comments were unjustified and regrettable. There is absolutely no connection between events in the UK and our business in Australia.''

Opposition communications spokesman Malcolm Turnbull defended Mr Murdoch and said the Prime Minister had an obligation to nominate the questions she thought needed to be answered by the Australian operation.

''There is no evidence of which I'm aware that that sort of phone hacking has been going on in Australia, whether by News Ltd journalists or anybody else,'' he said. ''If there was evidence of that, then again that is something the police should deal with.''

Australia's privacy laws have changed

http://www.dva.gov.au/footer/Pages/privacy_laws_change.aspx December 08, 2014

Australia's privacy laws will change on 12 March 2014. The new laws will apply to Australian Government agencies, private sector businesses and not-for profit ...

Australia's privacy laws changed on 12 March 2014. The new laws apply to Australian Government agencies, private sector businesses and not-for profit organisations covered by the Privacy Act 1988 (the Privacy Act). The changes to the Privacy Act include a set of new, harmonised, privacy principles that regulate the handling of personal information by both Australian government agencies and businesses. These 13 new principles are called the Australian Privacy Principles (APPs). They replace the existing Information Privacy Principles (IPPs) that previously applied to Australian Government agencies and the National Privacy Principles (NPPs) that applied to businesses.

Under the new laws it is easier for Australians to:

For more information about how DVA manages personal information and to access our Privacy Policy please visit www.dva.gov.au/privacy.htm.

For more information about the reforms and what they will mean for you, visit the Office of the Australian Information Commissioner (OAIC) website at www.oaic.gov.au.

The right to privacy

http://www.lawhandbook.org.au/handbook/ch21s05s01.php December 08, 2014

There are, broadly speaking, two types of privacy that may be protected by the law. The first type is personal information privacy, which means ensuring that ...

There are, broadly speaking, two types of privacy that may be protected by the law. The first type is personal information privacy, which means ensuring that individuals have enough control, choice, access to and understanding of how governments and businesses handle their personal information. The second type is the more general right to personal privacy, which is concerned with preventing parts of a persons private life from being made public.

Australian law does not generally protect the right to personal privacy, either in legislation or through the common law. Some cases in Australia have expressly recognised a common law right of action for a breach of an individuals right to privacy (see Grosse v Purvis [2003] QDC 151 and Jane Doe v Australian Broadcasting Corporation [2007] VCC 281); however, there has also been judicial commentary leaning in the opposite direction (see Kalaba v Commonwealth of Australia [2004] FCAFC 326; Giller v Procopets [2004] VSC 113 and Sands v State of South Australia [2013] SASC 44). Courts in the UK and elsewhere often look to duties of confidence when considering privacy issues (see Wainwright v Home Office [2003] UKHL 53 and Hosking v Runting [2005] 1 NZLR 1). However, see also Mosley v News Group Newspapers Limited [2008] EWHC 1777 (QB), which recognised privacy rights in the UK under the European Convention on Human Rights and Fundamental Freedoms.

The common law does provide some limited personal privacy protections, for example, through defamation and trespass laws (see Chapter 24.2: Defamation and Chapter 10.2: Neighbours and Noise). Some protection or relief may also be gained through obligations arising from the duty of confidence (see Chapter 19.1: Health Law).

There are also some very limited protections provided by legislation; for example, the Human Rights (Sexual Conduct) Act 1994 (Cth). (Also see Charter of Human Rights and Responsibilities Act 2006 (Vic) and the Human Rights Act 2004). In 2009, the NSW Law Reform Commission released a report entitled Invasion of Privacy. It recommended that the Civil Liability Act 2002 (NSW) be amended to provide a statutory cause of action for invasion of privacy. This report is available at www.lawlink.nsw.gov.au/lrc. In 2008, the Australian Law Reform Commission (ALRC) recommended a statutory cause of action be developed for serious invasions of privacy. A similar recommendation was made by the Victorian Law Reform Commission in its report entitled Surveillance in Public Places: Final Report, which was released in 2010. In September 2011 the Australian Government released an issues paper, A Commonwealth Statutory Cause of Action for Serious Invasion of Privacy, to inform its response to the Australian Law Reform Commissions recommendations. The paper considered whether Australia should introduce a statutory cause of action for privacy, and if so, what elements a statutory cause of action might include. The paper considered the analysis of the Australian, Victorian and New South Wales Law Reform Commissions, and the policy context and current legal positions in Australia and comparable jurisdictions. At the time of writing (July 2013) there has been no response to consultations.

There are far more significant protections for personal information privacy in Australia than the right to personal privacy. The protections are mainly provided through legislation. The most comprehensive information privacy legislation in Australia is the Privacy Act 1988 (Cth) (PA 1988). This sets minimum standards for the handling of personal information (in brief, information or an opinion about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion; see definition in s 6 PA 1988). The first set of standards apply to Australian and ACT Government agencies (see Information Privacy Principles (IPPs), below). Similar but separate standards apply to many private sector organisations (see National Privacy Principles (NPPs), below).

Significant reforms to the PA 1988 have been introduced by the Privacy Amendment (Enhancing Privacy Protection) Act 2012 (see Privacy Law Reform, below). The amending Act was given royal assent on 12 December 2012, however, most of the amendments will not take effect until 12 March 2014.

Since 21 December 2001, the coverage of the PA 1988 has extended to the private sector following the Privacy Amendment (Private Sector) Act 2000 (Cth). The amended PA 1988 established a co-regulatory regime based on the 10 National Privacy Principles that many private sector organisations must comply with. This regime also allows the development of privacy codes that the Australian Information Commissioner can approve (formerly approved by the Privacy Commissioner). While only a handful of codes are in place, an approved privacy code operates in place of the National Privacy Principles and is legally binding on the organisations that have agreed to apply it.

From 1 November 2010 the Australian Information Commissioner also has responsibility for administering other privacy related protections that were formerly performed by the Privacy Commissioner (as head of the OPC). These limit the collection, use and disclosure of information relating to old criminal convictions under the Crimes Act 1914 (Cth) (Crimes Act (Cth)), tax file numbers and some Medicare and pharmaceutical claims data under the National Health Act 1953 (Cth).

The Australian Information Commissioner Act 2010 (Cth) (AICA 2010) commenced on 1 November 2010. The AICA 2010 created a new independent agency, the Office of the Australian Information Commissioner (OAIC), which assumed the former OPCs regulatory role under the PA 1988. The OAIC brings together the functions of privacy protection, freedom of information (FOI) and government information policy across the Australian Government. The OAIC transition is therefore linked with changes to the Freedom of Information Act 1982 (Cth) (FOI Act (Cth)) (see Chapter 21.6: Freedom of Information). The OAIC has three statutory appointees: the Australian Information Commissioner as the agencys head, a Privacy Commissioner, and a new FOI Commissioner role. With the commencement of the AICA 2010, references in legislation to the former OPC, and the Privacy Commissioner as its head, now refer to the OAIC and the Australian Information Commissioner (as the new agencys head).

Some states and territories, including Victoria, also have information privacy legislation (see Victorian privacy legislation, below.) The Information

Privacy Act 2000 (Vic) applies to the management of all personal information except health information in the Victorian public sector. The Health Records Act 2001 (Vic) (HRA 2001) came into effect on 1 July 2002. Where the federal PA 1988 does not apply, the HRA 2001 will apply to personal health information held in the public and private sectors. However, in practice, private sector health professionals are often advised to comply with both the PA 1988 and state privacy laws.

Australian privacy law: swimming in the porridge of offshore disclosure

http://www.lexology.com/library/detail.aspx?g=61f5ad3e-95cf-4576-a128-c112278b2790 December 08, 2014

In the recent case of Professor Barry Spurr against the publishers of New Matilda, Federal Court of Australia Justice Michael Wigney was called upon…

In the recent case of Professor Barry Spurr against the publishers of New Matilda, Federal Court of Australia Justice Michael Wigney was called upon to apply the Australian Federal Act, the Privacy Act 1988, to restrain publication by New Matilda of Professor Spurr's emails. His Honour recounted his journey into the Privacy Act as follows: "A more labyrinthine, opaque piece of legislation I have yet to discover ... legislative porridge ... where almost every word is defined in ways that are counter- intuitive."

Having spent nine months grappling with Australian Privacy Principle (APP) 8, it is hard not to sympathise His Honour's frustration.

Since the Privacy Act was amended in March 2014 to include the Australian Privacy Principles, including APP 8 which regulates disclosures of personal information by Australian regulated entities to overseas entities, it has become commonplace for Australian regulated entities to seek privacy consents like the following:

We may disclose your personal information to X, Inc., an entity that provides services to us. X Inc.is not an Australian entity and is not regulated by the Australian Privacy Act 1988 and the Australian Privacy Principles (APPs) in that Act. By providing this Privacy Consent, you consent to the disclosure of your personal information to X, Inc. as an recipient outside Australia, on the basis that if X, Inc. engages in any act or practice that contravenes the APPs it would not be accountable under the Privacy Act and you will not be able to seek redress under the Privacy Act.

Such consents are sought by corporations and other businesses regulated by the APPs – so-called APP entities - with the objective of getting the APP entity within the APP 8.2(b) 'consent' exception (as discussed below). If successful, this exception operates to absolve the APP entity that collects the personal information and then discloses it to 'an overseas recipient' from accountability under section 16C of the Act for any act or omission by the overseas recipient which is contrary to the APPs. Accountability would otherwise arise through the curious interaction of APP 8.1 and section 16C of the Act. The provisions take quite a different approach to the European use of safe harbours and binding corporate rules. The operation of these provisions often gives rise to significant angst - and sometimes incredulity - of privacy counsel working outside Australia. The provisions are also quite odd when looked at closely.

Looking first at the outcome, privacy consents such as that above are drafted with an eye to the Australian Privacy Commissioner's Guidance as to the APP 8.2(b) exception, which at [8.28] states:

"At a minimum, this statement should explain that if the individual consents to the disclosure and the overseas recipient handles the personal information in breach of the APPs:

"APP 8.1 Before an APP entity discloses personal information about an individual to a person (the overseas recipient):

the entity must take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the Australian Privacy Principles (other than Australian Privacy Principle 1) in relation to the information.

Note: In certain circumstances, an act done, or a practice engaged in, by the overseas recipient is taken, under section 16C, to have been done, or engaged in, by the APP entity and to be a breach of the Australian Privacy Principles.

APP 8.2 Subclause 8.1 does not apply to the disclosure of personal information about an individual by an APP entity to the overseas recipient if:

Section 16C (Acts and practices of overseas recipients of personal information) provides:

(2) The act done, or the practice engaged in, by the overseas recipient is taken, for the

purposes of this Act:

So what is it about APP 8.1 and section 16C that leads to the incredulity of privacy counsel working outside Australia? Partly it is that the term 'overseas recipient' is not defined or explained in any meaningful way. An overseas recipient might be another APP entity which is not in Australia. More fundamentally, on one reading of APP 8.1, strict liability of the disclosing APP entity arises under section 16C regardless of whether the APP entity took reasonable steps to ensure that the overseas recipient does not breach the Australian Privacy Principles, or failed to do so. On this reading, despite having done everything it conceivably could do to protect privacy and assure that the overseas recipient does not breach the APPs, such as risk assessment and mitigation though appropriate operational controls and contractual measures and implementation of audit and review controls, an APP entity will be still strictly liable if the overseas recipient acts in a way that would have been a breach of the APPs if that act by the overseas recipient had been an act of the APP entity.

The availability of this reading leads most privacy lawyers to seek to avoid APP 8.1 by bringing an overseas disclosure with the exceptions in APP 8.2, of which the two exceptions quoted above are the most commonly used.

Why do so many APP entities collecting personal information seek to rely upon APP 8.2(b) and not APP 8.2(a)? Often it is because legal advisers will not express a view as to whether laws of a destination country have the effect of protecting the information in a way that is substantially similar to the way in which the APPs protect the information and provide adequate remedies. Such an opinion is difficult to give principally because it requires an in-depth knowledge of the privacy rules and remedies in two countries – and all other countries privacy rules, if not remedies, differ from Australia's (notwithstanding, in Asia Pacific, the existence of the so-called APEC Privacy Framework (available at www.apec.org)). Sometimes remedies in destination countries are quite different to remedies available under Australian law and their adequacy or otherwise cannot be the subject of a definitive opinion.

Often the problem is that the rules and remedies might look 'substantially similar' but those remedies are not clearly available to an Australian citizen because of jurisdictional obscurities. For example, personal health applications that enable an APP entity to disclose health information to a U.S. entity might be thought to have the benefit of the U.S. Federal law, The Health Insurance Portability and Accountability Act of 1996 (HIPAA Act) and privacy rules implemented pursuant to the HIPAA Act, which are suitably privacy protective. HIPAA will apply to U.S. entities covered by the law regardless of whether the personal health information they receive is from Australia or anywhere else, but not all health-related information is covered: it must originate from a healthcare-related transaction, and this leads to difficult questions (even leaving aside the further issue of how an Australian resident accesses remedies available under the HIPAA Act). And to date we have no assistance in the form of adequacy determinations by the Australian Privacy Commissioner, such as those of the European Commission in relation to such exotic destinations as New Zealand, the Faroe Islands and Uruguay. In any event, European determinations are one way only - from the European Union to the destination- and what matters for APP 8.2(a) is whether Australia considers the destination as having 'substantially similar' privacy protections and 'adequate' remedies.

So many APP entities seek instead to bring themselves within the APP 8.2(b) exception. But many privacy consents don't follow the Australian

Privacy Commissioner's Guidance, which arguably expresses the intended effect of APP 8.2(b) but really is a stretch from a literal reading of that provision. Some drafters bury the consent in a privacy statement that says words to the effect that If you consent to the collection by us and disclosure of your personal information to our overseas affiliate, APP 8.1 will not apply to the disclosure. By providing your personal information to us, you consent to our disclosure of your personal information to our overseas affiliate on that basis. This closely follows APP 8.2(b), but it is hardly 'transparent': would any individual (other than a privacy professional) register the risk and fully understand the effect of giving the consent?

Of course, the real concern is this: if an affected individual elects to read a privacy consent expressed in the form suggested by the Privacy Commissioner, it sounds quite dire. Are you really saying my personal information is off to Ruritania, there to be shopped to third parties and open to hackers and other miscreants? So drafters strive to soften the tone of the consent statement. And if, in fact, the practical effect of giving such a consent is not so dire, because the APP entity has done everything it conceivably could do to protect privacy by assuring that the overseas recipient does not breach the APPs, can the disclosing entity go on to describe what those steps were and why they should reassure the individual reading the form of consent? In policy terms, it makes sense to provide an affected individual with all the information that they reasonably need in order to give a fully informed consent. However, it is arguable that reassurances as to privacy protective measures may off-set the APP 8.2(b) privacy consent such that the individual is misled as to how to weigh whether to give the privacy consent.

This might all sound arcane, but it is a significant commercial issue. Remember that these individuals reading the privacy consent are usually the same individuals that deal online and through smartphones directly with offshore entities that are not effectively regulated in Australia (other than through operation of Australian Consumer Law) and often make florid but meaningless privacy claims that often are practically unenforceable both in Australia and in the destination jurisdiction. By contrast, Australian entities effectively underwrite compliance by off shore entities to whom personal information is disclosed, with that underwriting arguably complete and not qualified by the 'reasonable steps' language. So can an APP 8.2(b) disclosure include a description as to those reasonable steps without undermining the effectiveness of the exception? It remains to be seen, but in the meantime expect to see APP 8.2(b) exception-based privacy consents continue to multiply and expand in range and creativity.