Communications Law BULLETIN

CAMLA

Communications & Media Law Association Incorporated

Print Post Approved PP: 100001546

An Overview of Privacy Law in Australia: Part 1

In the first of a two part special, Peter Leonard provides a thoughtful commentary on privacy reforms. In this Part 1 he provides a high level overview of the amendments to the Privacy Act 1988 and the new Australian Privacy Principles. In Part 2 to be published in the next edition he provides an in depth analysis of Australia's privacy regime; focusing on the APPs, the regulation of privacy beyond the Privacy Act, issues of extraterritoriality and emerging trends and issues.

A quick guide to the changes

The *Privacy Act 1988* (the ***Privacy Act*** or the ***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. This Code also took effect on 12 March 2014.

The National Privacy Principles (***NPPs***) (for private entities, but subject to the small business exception) and Information Privacy Principles (***IPPs***) (for Federal government entities) are replaced with a single regime of privacy principles, the Australian Privacy Principles (***APPs***), which generally (but not universally) apply to Federal government agencies and private organisations alike.

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 that implementation is effective, repeatable and reliable. 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 the 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).

Volume 33 Nº 1
March 2014

Inside This Issue:

Contents

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:

From March 2014, the Commissioner's investigative and enforcement powers are significantly enhanced

- 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, which will be discussed in Part 2 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 Guidelines (the ***Guidelines***). These Guidelines are of significant interest as an expression of the Commissioner's interpretation of key provisions of the Privacy Act. The Guidelines are not given any express 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 does not appear to conform to a plain reading of corresponding provisions of the amending Act. Issues of interpretation are therefore likely to arise.

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. 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 behavioural 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 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 March 2014.

international law has had limited influence on the development of Australian privacy jurisprudence

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 *US 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.

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.

The APPs are arranged in the order of the personal information lifecycle, from collection, to use, to disclosure, to retention.

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.

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. Workplace surveillance, surveillance in public places, use of tracking devices, geo-tracking and recording technologies is currently regulated by state and territory statutes that are diverse and inconsistent.

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 codes 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.

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 OAIC is responsible for enforcing compliance with the Privacy Act and reviewing proposed privacy codes

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 diagram on page 6.

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.

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.

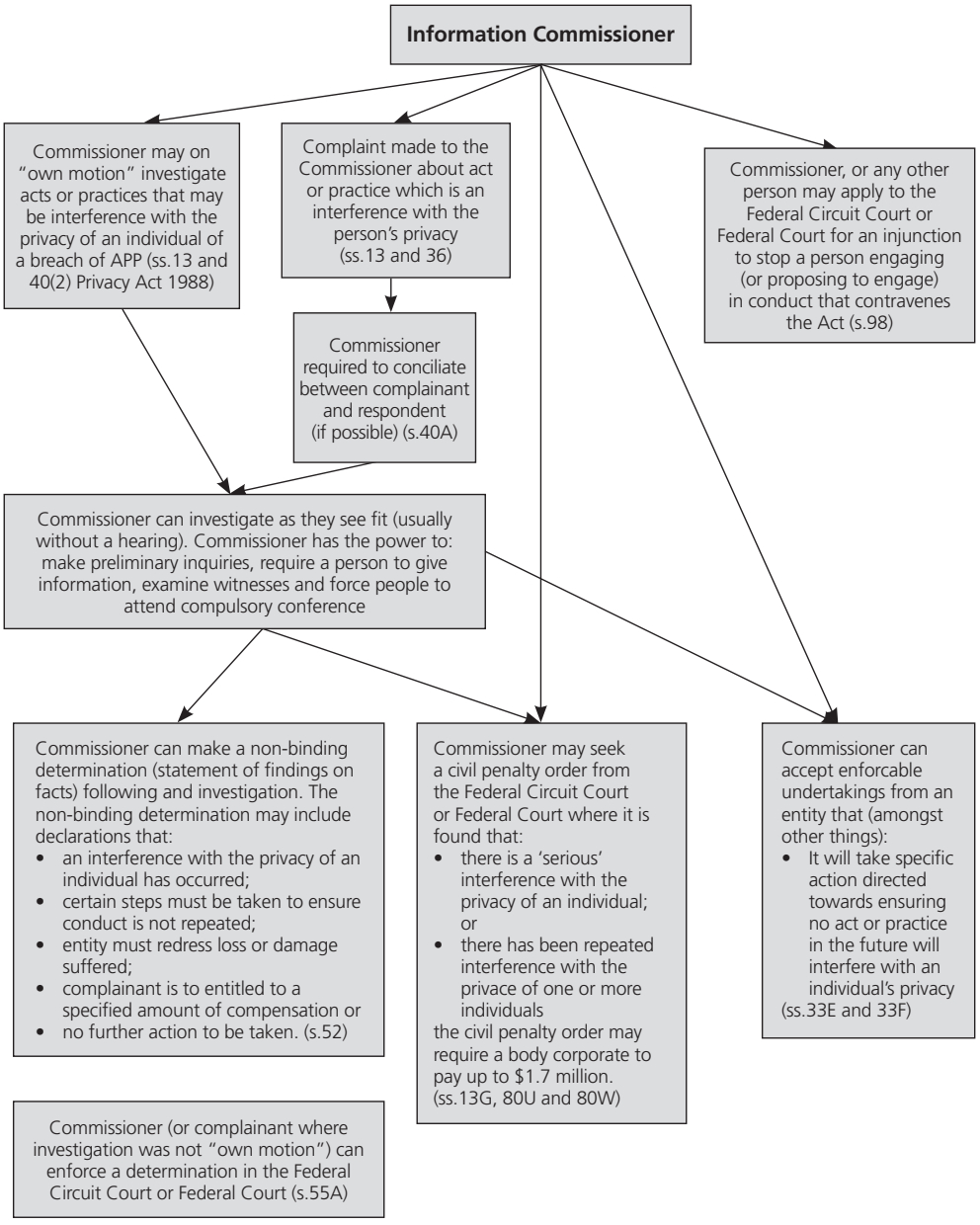
This partial exemption for related bodies corporate also does not apply in a range of circumstances, including (but not only) the collection or disclosure of 'sensitive information'; the collection of personal information from an entity that is exempt from the Privacy Act; where the company is a contractor 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.

Part 2 of this article will appear in the next edition of CLB.

Peter Leonard is a partner at Gilbert+Tobin Lawyers and a director of the International Association of Privacy Professionals ANZ (iappANZ).



Does Australia Need a "Right to be Forgotten"?

As issues of internet privacy receive increasing attention around the world, Jarrod Bayliss-McCulloch draws on the experience overseas and explores the tension between the individual's right to privacy in the online world and the right of third parties to freedom of expression. He considers whether a statutory "right to be forgotten" would be appropriate in the Australian context.

Introduction

On 24 January 2014, a Hamburg court ordered Google Inc. to block search results linking to photos of a sex party involving former Formula One boss Max Mosley from its website in Germany.[1] This is only the latest in a long series of legal actions Mosley has brought in relation to the photos across multiple jurisdictions, and comes after a French court ordered Google to find a way to remove recurring links to images of Mosley on 6 November 2013.[2]

It is not hard to understand why Mosley wanted the photos removed. The images showed him engaging in sexual practices and were sourced from a news story, published back in 2008 in News Corporation's now-defunct *News of the World* Newspaper, which alleged he had organised a "sick Nazi orgy",[3] a claim later shown to be defamatory. Mosley was awarded 60,000 pounds (US $99,800) in damages by an English court as a consequence of that story. The Court ruled the alleged Nazi theme had no foundation in fact and that the story was not in the public interest. Mosley received a similar ruling in France in 2011 when a judge ordered News Corporation to pay 32,000 euros in fines and fees in relation to the story.[4]

In the latest episode of this saga in Hamburg, the Court has ruled that while Google did not take the pictures, it was responsible, as a distributor, for linking its search results to a page that housed the images. In making the order for Google to block images of Mosley from its search results the Court appears to have taken into account the graphic and damaging nature of the content involved;[t]he banned pictures of the plaintiff severely violate his private sphere, as they show him active in sexual practices" the court said.[5] Was this in fact the *right* [legal] outcome? This question will be discussed later in the article, but for present purposes the whole Mosley scenario raises several poignant questions that help to frame the issues around a "right to be forgotten."

When even a wealthy, highly respected business person living in a region of the world that is renowned for its strong privacy protections has to fight through years of intense and costly legal battles in multiple jurisdictions for the right to remove private material from the internet that has been illegally published, there is something wrong with the system. Is it a sign that technology's reach has exceeded the law's grasp? Do individuals need a more explicit right to be forgotten in the online world? If so, how would such a right be enforced?

There is an old Jewish tale that illustrates the struggle we are increasingly grappling with these days concerning the flow of information. It likens the lies told by a man about a Rabbi in the village to pillow feathers blown about by the wind, which are later all but impossible to gather. Variations of this story have been used for centuries to demonstrate the harm of careless words and their impact on a person's reputation. The story finds new relevance today, where words fly on the wings of the internet to the most distant parts of the world, before coming to rest in a permanent record. As we increasingly spend time and energy communicating online, embracing the power of user-generated content and interactive experiences, we cast more feathers to the wind: blog entries, status updates, tweets, text, images and video. The average social network user receives 285 pieces of content daily, including 54,000 words and 443 minutes of video.[6]

Google does not have to remove legal and correct personal information from search results, even if that information is damaging to an individual's reputation, because this would "entail an interference with [its] freedom of expression."

Importantly, today these feathers are not simply scattered to *the wind*. "Once [data] is out there, it's hard to control."[7] Content may be duplicated and replicated on multiple sites. It may be indexed and searchable, in a fraction of a second in one of the 1.2 trillion Google searches conducted every year. Indeed, "today it is easier and cheaper to remember than it is to forget. This can have a big impact on people's lives,"[8] as Mosley's experience bears out.

---

1 Reuters, *German court orders Google to block Max Mosley sex pictures* (Frankfurt, 24/1/2014), http://www.reuters.com/article/2014/01/24/us-google-germany-court-idUSBREA0N0Y420140124, accessed 21/2/2014.

2 CNET, *Privacy ruling forces Google to delete racy images* (6/11/2013) http://news.cnet.com/8301-1023_3-57611176-93/privacy-ruling-forces-google-to-delete-racy-images, accessed 21/2/2014.

3 Reuters, see above n1.

4 Bloomberg, *Google Inc told 'Nazi-themed' orgy images linked to Max Mosley must be blocked from search results in Germany* (24/1/2014) http://business.financialpost.com/2014/01/24/google-inc-max-mosley/?__lsa=5be3-f5f9, accessed 21/2/2014.

5 Reuters, see above n1.

6 IACP Center for Social Media, (2013) 'Fun Facts', http://www.iacpsocialmedia.org/Resources/FunFacts.aspx#sthash.YB2KT47e.dpuf, accessed 30/10/2013.

7 Jonas, J., in Thierer, A., (2011) 'Erasing Our Past On The Internet', *Forbes*, 17/4/2011, http://www.forbes.com/sites/adamthierer/2011/04/17/erasing-our-past-on-the-internet, accessed 29/10/2013.

There have been numerous recent international developments in this area. In September, the State of California introduced a bill that will allow minors to ask websites to remove personal content.[9] In Europe, the European Commission continues to debate how the "right to be forgotten" should practically be enforced through its data protection regulations.[10] In Australia, the Australian Law Reform Commission (***ALRC***) is currently considering whether Australia should adopt a right to be forgotten to address privacy problems on the internet,[11] including "a requirement that organisations, such as social media service providers, permanently delete information at the request of the individual who is the subject of that information."[12]

Formulating a "right to be forgotten" requires balancing interests in freedom of expression with the right to privacy, concepts deeply informed by cultural sensitivities, as the Californian and European experiences demonstrate. Beyond this lies a significant technical question: whether it is even possible to enforce such a right in an open system like the internet.

In considering whether an explicit right to be forgotten would be beneficial in such cases, it is important to keep in mind also that Australian law already provides recourse in many situations where illegal content is posted online, without a specific right to be forgotten

Privacy considerations and the rights of the individual

In theory, the right to be forgotten addresses a serious problem in the digital age. People "often self-reveal [online] before they self-reflect and may post sensitive personal information about themselves - and about others - without realizing the consequences."[13] Proponents of a right to be forgotten point to examples like President Obama, who wrote about drug use in his autobiography *Dreams of My Father*,[14] or current litigants like Max Mosley. Although the case of Obama is hypothetical because graphic evidence of his drug use as a youth never entered the public domain, we can speculate about the devastating consequences that content about a person's youthful indiscretions could have if seen by a potential employer or political opponent, even decades after the event. The proliferation of private content about a person's more recent indiscretions as an older person, as in Mosley's case, can be even more harmful.

"Dignity, honour, and the right to private life" are recognised among the most important fundamental rights for Europeans,[15] and Europe has a history of protecting individuals from such harm, traditionally prioritizing people over media and technology companies.[16] The intellectual origins of the right to be forgotten are seen in the French *droit à l'oubli*, and the modern day laws of Switzerland,[17] which allow a rehabilitated criminal to object to the publication of the facts of his conviction.[18] The underlying premise is that criminals do not remain of public interest forever, so the public should not have access to their criminal records indefinitely.

There is, however, an important distinction to be drawn here. Publication of a rehabilitated criminal's reasons for conviction is a serious matter, with the potential to incite ongoing prejudice against an individual who has already made atonement in the eyes of the law. It is also a different thing entirely from the retention of information once expressed by an individual in the public domain from which he or she later wishes to resile . In each example the individual has a clear interest in having injurious content removed from public viewing but in the latter case, the harm is of a different nature; rather self-inflicted and arguably deserving less sympathy in the eyes of the law. When discussing the scope of the right to be forgotten, however, European Commissioner Reding applied the historic principle to such modern day situations, noting particular risks for teenagers in revealing compromising information they may later regret.[19]

Importantly, the notion of protecting the individual is not as pronounced in Australia's privacy laws as those articulated in Europe. Australia has no historical equivalent of the right to be forgotten. Nor is there any general right of an individual to privacy. Rather Australia's privacy law provides strong protections when it comes to the handling of personal information, and it would not be entirely out of character for the Australian legislature to strengthen individual rights further in the online world. After all, it is a world where the individual is structurally disadvantaged, with little say in how personal data is distributed. Powerful online operators impose standard terms granting them broad rights over user content.[20] Individuals retain limited control over data once they "agree": a prerequisite to accessing platforms which are increasingly seen as essential to modern life.

---

8 Selby, J., in Clark, L., (2013) 'Should we have a right to be forgotten?', *Bandt*, 17/10/2013, http://www.bandt.com.au/news/digital/should-we-have-a-right-to-be-forgotten, accessed 31/10/2013.

9 California Senate Bill No. 568, Chapter 22.1 "Privacy Rights for California Minors in the Digital World", available online at http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB568, accessed 29/10/2013.

10 See for example, European Commission, (2012) *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, 25/1/2012, http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf, accessed 28/10/2013.

11 Australian Law Reform Commission (2013), *Serious Invasions of Privacy in the Digital Era: Issues Paper 43*, October 2013, http://www.alrc.gov.au/publications/invasions-privacy-ip43, accessed 29/10/2013.

12 Ibid, at para 170.

13 Steyer, J., (2013) 'Why Kids Need an "Eraser Button"', Common Sense Media, 19/9/2013, http://www.commonsensemedia.org/blog/why-kids-need-an-eraser-button, accessed 29/10/2013.

14 Selby, J., in Clark, L., see above, n. 3.

15 Weber, R. H., (2011) 'The Right to be Forgotten: More Than a Pandora's Box?' 2 (2011) JIPITEC 120, at 121, para. 5.

16 Consider for example the 19th Century case involving famous French author Alexandre Dumas, Dumas, 13 A.P.I.A.L. at 250 ("[L]'effet même de la publication . . . que si la vie privée doit être murée dans l'intérêt des individus, elle doit l'être aussi souvent dans l'intérêt des moeurs . . . ." in Whitman, J. "The Two Western Cultures of Privacy: Dignity Versus Liberty" 113 Yale Law Journal 1153, at 1176, http://www.yalelawjournal.org/images/pdfs/246.pdf, accessed 30/10/2013.

17 See for example, Swiss Federal Court, October 23, 2003, 5C.156/2003.

18 Rosen, J., (2012) 'The Right to be Forgotten', 64 *Stan. L. Rev. Online* 88 (13/2/2012), http://www.stanfordlawreview.org/online/privacy-paradox/right-to-be-forgotten, accessed 29/10/2013.

19 Reding, V. (2012) 'The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age' 5 (Jan. 22, 2012), http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/26&format=PDF, accessed 30/10/2013.

20 Chow, E., (2013) 'Learning from Europe's "Right to be Forgotten"' The Huffington Post, 9/9/2013, http://www.huffingtonpost.com/eugene-k-chow/learning-from-europes-rig_b_3891308.html, accessed 29/10/2013.

Thus the Australian legislature may have some interest in strengthening the rights of vulnerable individuals to remove damaging content from the online environment. However such measures must be reasonably adapted to preserve other fundamental rights they may inadvertently erode, including freedom of expression.

Freedom of expression and the right to be forgotten

Three broad variations of the right to be forgotten pose progressively greater threats to the right to freedom of expression.[21] The first of these Fleischer describes as the "right to access and rectify one's own personal data."[22] This is nothing new to Australian law, and is not particularly controversial. Indeed the individual's right to access and correct personal information is already reflected in various privacy principles under the *Privacy Act*.[23] This "data minimisation" approach poses little threat to freedom of expression. [24]

By contrast, if the right is viewed "more sweepingly as a new right to delete information about oneself, even if published by a third-party"[25] (including photos, blogs or third party content) , the idea that the law should support this right would be troubling. In a world where freedom of expression may attach to minor expressions such as a click of a "like" button,[26] any such extension of the law sets the individual's right to be forgotten on a collision course with the third party's right to share and discuss information. A whole new body of law would need to be developed to determine when and in what circumstances one right should prevail over the other. In the meantime, the service provider would have to act as arbiter, under the shadow of penalties and uncertainty as to the true meaning of the law. As Rosen observes, "Facebook [would] have to engage in…difficult line-drawing exercises... and [with] the prospect of ruinous monetary sanctions…opt for deletion in ambiguous cases, producing a serious chilling effect."[27] This chilling effect may be even greater in Australia, where freedom of expression is a "precarious freedom" that relies on a common law tradition rather than an entrenched statutory or constitutional protection.[28]

Fleischer's third and most extreme interpretation of a right to be forgotten goes even further, extending to require deletion of content merely linked to by a third party.[29] On this issue, the European Court of Justice (ECJ) is currently considering the complaint of a Spanish man who discovered records of an auction of his property (which stemmed from a legal notice published in a newspaper) could be found on Google. [30] The man asked for this information to be deleted and the Spainish courts upheld the complaint, but Google refused to comply.

In a non-binding opinion the ECJ's adviser stated that Google does not have to remove legal and correct personal information from search results, even if that information is damaging to an individual's reputation, because this would "entail an interference with [its] freedom of expression."[31] This resonates with Google's view that requiring search engines to suppress "legitimate and legal information" would amount to censorship.[32] This principle, that imposing an obligation to block access to *legally-published* content would dangerously interfere with freedom of expression and users' rights to access information, as well as a search engine's right to do business, is equally valid in the Australian context.

Of course, there are times when information is published online *illegally*. An important question then arises as to whether merely *linking* to illegal information published by a third party should be illegal, or at least a circumstance in which an innocent third party whose information is linked to by a search engine should have a legal remedy to have such a link removed from the search engine's index.

Hypothetically, even if a search engine were to delete all links to the illegal content held on all third party pages at a given point in time, there is no guarantee that somewhere, somebody has not stored a copy of the illegal content

This is the issue that was raised in Mosley's (multiple) claims against Google identified at the outset of this paper. Those circumstances are very different from those at play in the ECJ case; auction results for a property transaction involving an ordinary member of the public seem rather innocuous when compared to sex photos of a public figure published in the context of an alleged "nazi-themed" sadomasochistic orgy. For Mosley, the stakes were immensely higher; the potential harm immeasurably greater. It is easy to say that he *should* not have to suffer harm as a result, whether of primary publication, secondary publication or third party links to such content. As a practical matter, were it not for Google's role in linking to those images, very few people would ever see that content, and consequently, Mosley would suffer very little harm;; Google is therefore at least somewhat to blame for the harm he suffered and should be held accountable.

There is no denying that Google is very powerful. The vast and labyrinthine structure of the internet makes us all so reliant on search engines like Google to navigate it. Living in the information age, a world where the old maxim "knowledge is power" resonates more deeply than ever before, we have a special vulnerability in this respect, as Google increasingly becomes our primary portal for gathering information. It is this power, stemming from Google's dominant execution of its core search capability, that recently propelled Google briefly to surpass Exxon Mobil as the second most valuable US company by market capitalisation.[33]

The law has long had an important role in protecting the weak from the powerful, and this principle applies equally in the case of

21 Fleischer, P., see above, n. 8.

22 Ibid.

23 Consider the application of Australian Privacy Principles 12 and 13, which will come into effect in March 2014.

24 Fleischer, P., see above n. 8.

25 Ibid.

26 *Bland v Roberts* No. 12-1671, 2013 WL 5228033 (4th Cir. Sept. 18, 2013).

27 Rosen, J., see above, n. 16.

28 Gelber, K., (2003) 'Pedestrian Malls, Local Government and Free Speech Policy in Australia', (2003) 22(2) Policy and Society: Journal of Public, Foreign and Global Policy 23.

29 Fleischer, P., see above, n. 8.

30 *Google Spain S.L. and Google Inc. v Agencia Española de Protección de Datos, Case C-131/12*.

31 Opinion of Advocate General Jääskinen, *Case C-131/12*, (25 June 2013), at 134, http://curia.europa.eu/juris/document/document.jsf?text=&docid=138782&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=11341#Footnote1, accessed 2/11/2013.

32 Echikson, W., (2013) 'Judging freedom of expression at Europe's highest court', (26 February 2013), http://googlepolicyeurope.blogspot.co.uk/2013/02/judging-freedom-of-expression-at.html, accessed 3/11/2013.

Google. Yet it is important to remember that although powerful, Google is not omnipotent. It remains bound by the same constraints as the rest of us when it comes to the fundamental nature of the internet. For this reason, the decision of the Hamburg court may not be the *right* one and perhaps despite initial appearances Mosley's should not be an open and shut case.

After balancing interests in privacy and freedom of expression, a limited right to be forgotten may be appropriate given the permanence of online records and their potential impact on an individual's life and employment prospects

Google of course, is one step removed from News Corporation. Google did not take the pictures and publish them, nor did it download the pictures from the News Corporation website and deliberately or conscientiously republish them on a separate website. All it did was link to content, which had been republished by a third party. After all, Google is a search engine, a content aggregator. That is what Google does. It trawls the internet indexing content and creating links so that we can have the information we want available at our fingertips whenever we want it. We take it for granted these days, but that is a phenomenal achievement, because the internet is a big place. Almost incomprehensibly so. When I type "Free Speech" into Google, "about 1,060,000,000" results are returned. The task of proactively identifying a web page containing illegal sex pictures of a particular individual, from amongst the billions of web pages Google indexes, with a view to plucking that page out of Google's vast and complex repository of data, puts the old metaphor of "searching for a needle in a haystack" to shame. Should a search engine like Google really be responsible for proactively monitoring even the smallest components of the enormous and constantly changing, writhing mass of content it transmits and stores for its users?

Perhaps this is why the French court, in Mosley's case in November 2013, only ordered Google to pay 1 Euro (US $1.37) in damages despite finding in Mosley's favour. Perhaps the French court was also influenced by the fact Google, like other search engines are generally cooperative and responsive when met with take down requests seeking for them to remove illegal content. Indeed, in a blog post published in September, Google said it had already removed "hundreds of pages for Mr. Mosley" as part of a process that helps people delete specific pages from Google's search results after they have been shown to violate the law.[34] The fact that there were only nine pages left for the court to order Google to remove at the time the case reached the French court, and a mere 6 in Germany, suggests that Google's internal processes were at least largely effective in allowing Mosley to remove damaging content from its links.

In considering whether an explicit right to be forgotten would be beneficial in such cases, it is important to keep in mind also that Australian law already provides recourse in many situations where illegal content is posted online, without a specific right to be forgotten. The tort of defamation provides civil remedies and injunctive relief for publication of material that exposes a person to ridicule or injures their reputation. In addition, the expanding common law principles of breach of confidence[35] protect individuals from harm including emotional distress[36] suffered from disclosure of confidential information. These causes of action are not limited in their application to online matters; harmful content that causes harm can and should be removed from source websites under existing law. Once so removed, the content will also disappear from a search engine's index, rendering a further "right to be forgotten" unnecessary.

Yet the Google experience shows that the debate around the right to be forgotten may be raising false expectations in the community.[37] Fleischer reports receiving "requests from people to 'remove all references to me…from the Internet.'"[38] Such sweeping requests are not only unrealistic in the context of the online world, but they raise questions about how the right should be balanced against the public interest in accountability, journalism, history, innovation and scientific inquiry.[39] Should political figures be able to request removal of reports containing views they no longer hold? Should the author of a scientific study be able to request withdrawal of the publication? Who should decide, and under what principles?[40] These questions highlight the risk that an extensive right to be forgotten could undermine the preservation of history, the individual and collective memory of society,[41] and "may [even] lead to 'the society that was forgotten'."[42]

The practical difficulties of enforcing a "right to be forgotten"

Even if the benefits of a right to be forgotten in protecting individual privacy were found to outweigh the threat it poses to freedom of expression, a "purely technical and comprehensive solution to enforce the right in the open Internet is generally impossible."[43]

The fundamental technical challenges in enforcing a right to be forgotten are fourfold:

(i) identifying and locating all personal data items;

(ii) tracking all copies of an item and of information derived from it;

(iii) determining a person's right to request removal of data; and

(iv) effecting the removal of all exact or derived copies of the item, once authorised.[44]

The third challenge may be addressed through clear drafting of the statutory provision giving the right to request removal of data, assuming it is possible to specify with precision the exhaustive circumstances in which the right may be exercised. This seems doubtful

33 B. Womack, *Google Briefly Tops Exxon as 2nd-most valuable US Firm* (Bloomberg, 8/2/2013), http://www.bloomberg.com/news/2014-02-07/google-passes-exxon-to-become-second-most-valuable-u-s-company.html, accessed 24/2/2014.

34 Reuters, see above n1.

35 See *Giller v Procopets* [2008] VSCA 236.

36 In *Giller v Procopets* [2008] VSCA 236, the Victorian Court of Appeal awarded damages for emotional distress for breach of confidence, in cases where that action is akin to a tort of "misuse of private information".

37 Fleischer, P., see above n. 8.

38 Ibid.

39 European Network and Information Security Agency (ENISA) (2011) 'The right to be forgotten - between expectations and practice' (18/10/2011), at 12.

40 Ibid.

41 Beckles, C., (2013) 'Will the Right to be Forgotten Lead to a Society that was Forgotten?' *IAPP* (14/5/2013), https://www.privacyassociation.org/privacy_perspectives/post/will_the_right_to_be_forgotten_lead_to_a_society_that_was_forgotten, accessed 2/11/2013.

42 Ibid.

43 ENISA, see above, n. 36, at 7.

44 Ibid, at 13.

considering provisions proposed in other jurisdictions and the challenges involved in reliably anticipating the ongoing development of new technologies and means of distributing information.

The remaining challenges are even more difficult to resolve. They relate to the underlying information system. Specifically, the ability to enforce a right to erasure is technically feasible only in 'closed' systems that reliably account for the processing, storage and dissemination of all information, in which all participants are linkable to real-world entities located in jurisdictions that enforce the right.[45]

In an open system like the internet, anyone can make copies of public data items and store them at arbitrary locations, on an anonymous basis, without copies being tracked. This activates the first and second challenges identified above: it is not generally possible for a person to locate and track all personal data items (whether exact or derived) stored about them.[46] Even if the right to request removal of a data item is granted, the fourth challenge arises: like feathers scattered to the wind, no single entity will have the authority or practical ability to delete all copies. Generally speaking, enforcing the right is impossible in an open, global system.[47]

Regardless of the nature of the underlying system, "unauthorized copying of information… is ultimately impossible to prevent by technical means";[48] personal information stored offline, on tape archives or flash devices, cannot easily be located or removed, representing another practical barrier to enforcing a right to be forgotten.

This is part of the challenge faced by Google and other search engines as prospective arbiters of the "right to be forgotten" in relation to content which has already been declared illegal, as in the case of Mosley. Hypothetically, even if a search engine were to delete all links to the illegal content held on all third party pages at a given point in time, there is no guarantee that somewhere, somebody has not stored a copy of the illegal content. In fact, as a practical matter, it is almost guaranteed that somewhere in the world, somebody *will* have a copy of the illegal content, whether on their iPad or portable storage device or even cached on their personal computer. There is nothing to stop such a person from posting that content online again, at which point the process of syndication, replication and indexing can start all over again. The result is a never-ending game of catch up played out on a global scale that technology giants struggle to keep up with based on current innovations and the law can never hope to win.

Conclusion

After balancing interests in privacy and freedom of expression, a limited right to be forgotten may be appropriate given the permanence of online records and their potential impact on an individual's life and employment prospects. The right, however, should be limited to the least intrusive conception identified by Fleischer and the protection of particularly vulnerable groups.

This was the view adopted by the Californian legislature in SB 568. Unlike the broad principles proposed in Europe, which risk intruding on freedom of expression, the Californian law is less extensive. It protects only minors who are registered users of a website, giving them rights to request deletion of their own posts and not posts of third parties. One may query whether similar regulations are required at all in Australia, given the majority of websites already afford users the ability to control information they have uploaded. Legislating beyond this, to enforce the second or third conception of the right, would impose unacceptable constraints on freedom of expression in Australia. It would also be unnecessary given other remedies available to individuals to remove harmful content under existing law.

Remember the tale of the feather pillow. It is generally easier to avoid casting feathers in the first place than to gather and return them to the pillowcase. This is particularly true when it comes to distributing information across an open network like the internet. Perhaps the key then is education and personal responsibility.

While the right to privacy in the online world is important, so is freedom of expression. Let us not forget one of the greatest collective benefits the internet affords society. The right to have its many voices heard, no matter how remote; the chance for its citizens to be remembered, for all the right reasons.

The internet is not a risk-free playground but an extension of the real world, in which discretion must be exercised. With this in mind, perhaps we can avoid the need for an extensive right to be forgotten in Australia and allow freedom of expression to flourish, to the enduring benefit of society.

Jarrod Bayliss-McCulloch is a lawyer at Baker McKenzie. Jarrod won the 2014 CAMLA Young Lawyer essay competition with an earlier version of this article.

45 Ibid, at 13.
46 Ibid, at 15.
47 Ibid, at 13.
48 Ibid, at 13.

'Australia's Privacy Principles and Cloud Computing: Another Way'

Kanin Lwin considers the application of the new APPs to the cloud computing industry.

Telecommunications advances, assisted by the development of the Internet, have spawned enormous opportunities for sophisticated data exchanges and has led to the proliferation of data outsourcing arrangements, especially cloud computing. These developments have, however, also made it easier for organisations to harvest and disseminate large quantities of personal information.

Privacy regimes in certain countries balance the interests of individuals in protecting their personal information with the economic efficiencies generated through data outsourcing, by distinguishing between entities that *control* how and what personal information is processed (***controllers***) and entities which merely process data on behalf of a controller (***processors***).

In many although not all situations, cloud providers will not be collectors or controllers of personal information

By contrast, the new Australian Privacy Principles (***APPs***), which will replace the National Privacy Principles (***NPPs***) and Information Privacy Principles (***IPPs***), do not purport to make such distinctions, despite applying to the lifecycle of collection, handling and destruction of personal information.[1] Consequently, the APPs have been criticized[2] for exposing cloud providers, in those instances where they act only as processors of personal information, to privacy obligations which may be beyond their capacity to comply.

This essay will contend, however, that the regulatory, economic and practical considerations surrounding cloud computing create a strong contextual impetus for reading the APPs in a way that recognises that providers and customers can and do have different roles in the processing of personal information. In particular, it will argue that many APPs, as a result of their operation, do in fact distinguish between (i) 'collectors' and 'non-collectors' of personal information and (ii) 'controllers' and 'processors'.

Background

Regulatory landscape

The marriage of computer and telecommunications technologies has spurred the evolution of automated message transmissions and enabled vast movements of data. In particular, the Internet has increased the possible scale and complexity of data interchange: already, internet traffic exceeds 1.5 billion gigabytes each day.[3] Whilst the opportunity for greater data flows has unlocked considerable economic benefits for society in general, it also poses significant privacy risks to individuals.

Economic Benefits

Businesses can now harness powerful communication networks to process their data externally, thereby tapping into an outsourcer's pool of resources along with the accompanying cost efficiencies. Cloud computing, for example, describes an arrangement wherein clients outsource some or all of their information technology (***IT***) workload by using the Internet to access, on demand, 'a shared pool of configurable computing resources (eg. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction'[4] (***cloud***).

The extent to which clients manage the underlying IT resources depends on the model selected; greatest control exists in an 'Infrastructure-as-a-Service' arrangement, and the least control in 'Software-as-a-Service' with 'Platform-as-a-Service' in between. One attraction of the cloud is that clients consume computing resources as a service, renting only as much of the provider's infrastructure as required, and thus can leverage off the considerable economies of scale consolidated within provider data centres.

Privacy challenges

However, the corresponding erosion of the individual's ability to control the circulation of information about themselves, a popular although not undisputed description of privacy,[5] threatens to offset these commercial benefits.

Communications and networking technology make it increasingly feasible for organisations to disseminate large quantities of personal information, often without an individual's knowledge or acceptance. Moreover, the 'Internet age' has spawned a situation where social interactions are fast becoming online affairs,[6] aggravating existing privacy concerns.

With growing amounts of information coursing through the Internet, it has become far easier for organisations to collect private information about customers and their personal habits, increasingly valuable commodities in today's information-driven economy[7]. By one estimate, the top 50 websites install on average 64 pieces of tracking software onto a person's computer, usually without warning, inhibiting an individual's control over their personal information.[8]

---

1 Explanatory Memorandum, *Privacy Amendment (Enhancing Privacy Protection) Bill 2012* (Cth), 52 ***(Explanatory Memorandum).***

2 James North and Daniel Thompson, 'Privacy Laws Are Affecting Australia's Cloud Industry', *Corrs Chambers Westgarth Thinking,* http://www.corrs.com.au/thinking/insights/privacy-laws-are-affecting-australias-cloud-industry/ 7 March 2013

3 Jeff Jarvis, *The Guardian* (online), http://www.theguardian.com/commentisfree/2013/aug/13/nsa-internet-traffic-surveillance 13 August 2013

4 Peter Mell and Timothy Grance, 'The NIST Definition of Cloud Computing', (Special Publication 800-145, National Institute of Standards and Technology, United States Department of Commerce, September 2011), 2.

5 Daniel Solove, *Understanding Privacy* Harvard University Press, (1st ed, 2008) 24-29.

6 McKay Cunningham, 'Diminishing Sovereignty: How European Privacy Law Became International Norm' (2012) 11 *Santa Clara Journal of International Law* 423.

7 Horace Anderson, 'The Privacy Gambit: Toward a Game Theoretic Approach to International Data Protection' (2006) 9(1) *Vanderbilt Journal of Entertainment and Technology Law* 5.

8 Cunningham, above n6, 426.

Furthermore, much of the value in personal information lies as part of larger value-added assets like the database of customer payment information facilitating Amazon.com's '1-Click' payment system wherein customers can make online purchases through a single mouse click, without needing to re-enter their billing details.[9] Organisations are thus incentivised to accumulate ever expanding dossiers on individuals, perpetuating ever greater intrusions into the private sphere.

Reaching a balance

To accommodate both the economic benefits of allowing greater data traffic and providing adequate protections against organisations mining this data traffic for personal information certain privacy regimes distinguish between controllers and processors. Singaporean legislation for instance exempts 'data intermediaries' (effectively another name for 'processor') from most privacy law responsibilities.[10]

The reason for this functional distinction is twofold. First, the concept of 'controller' gives individuals an entity against whom they can enforce their privacy rights, thereby re-asserting some control over the circulation of their personal information. The European Union, as an example, requires controllers to ensure an individual's right of correction is delivered in practice.[11] Secondly, the existence of 'processors' as separate entities handling information on the controller's behalf recognises that the controller's responsibility for the processing of personal data does not mean controllers must always physically handle personal information. Thus it accommodates for the practical reality of data outsourcing.

APPs

The APPs purport to recognise that 'protection of the privacy of individuals is balanced with the interests of entities carrying out their functions'[12], therefore they address to some extent the competing considerations influencing privacy protection design. However, the APPs seem to allocate responsibilities irrespective of the functional differences between data processing participants and so might not in fact effectively balance between securing the privacy interests of individuals and the economic benefits inherent to outsourcing arrangements.

With respect to the private sector, the APPs will apply to any 'organisation' depending on whether that entity:

- 'Collects',[13] 'holds',[14] 'collects and holds'[15] ,'receives',[16] or 'discloses',[17] personal information;
- 'Adopts' or 'uses/discloses' a government-related identifier;[18]
- 'Deals'[19] with an individual; or
- Is an 'APP entity'.[20]

One possible explanation of this approach could be a desire to shift the focus away, in many instances, from what entities are and onto what entities do with personal information, especially given entities can alternate between acting as controllers or processors when processing data[21]. Nevertheless, from the standpoint of cloud arrangements, the APPs, on face value, encounter significant practical, regulatory and commercial difficulties.

Cloud providers as processors & non-collectors

In many although not all situations, cloud providers will not be collectors or controllers of personal information. For example, clients who leverage a cloud solution to scan their emails for malware are usually responsible for setting, via the management console under their control, the directions according to which that data is processed.[22] With such solutions, the cloud provider should also generally have administrative and process locks in place to help ensure they remain, on a day to day basis, at arm's length from the data running through their infrastructure.[23]

Even if cloud providers can be said to hold data that resides on their servers, insofar as entities 'hold' personal information under their possession or control,[28] they often lack the capacity to provide access

The Australian Information Commissioner (***Commissioner***) has also released guidelines for the APPs (***Guidelines***) which state that, subject to certain conditions, clients may be regarded as controlling personal information where their cloud agreement empowers them to determine how data is processed[24].

The Guidelines are not legally binding, however, the Commissioner will take the Guidelines into account when applying the APPs.[25] And the Commissioner's guidance in relation to control by contract replicates earlier guidance regarding the IPPs.[26]

In certain situations, however, cloud providers will act as collectors and controllers, such as where a provider harvests personal information from emails stored on their cloud solution.[27]

Practical

One practical problem of applying all the APPs to each data processing participant is that given cloud providers often act as processors and non-collectors, they would frequently need to adhere to many

9 Anderson, above n7.

10 *Personal Data Protection Act 2012* (Singapore) ss2(1) and 4(2).

11 Article 29 Data Protection Working Party, *Opinion 1/2010 on the concepts of 'controller' and 'processor',* EU Doc 00264/10 EN WP 169 (adopted 16 February 2010) 4 (***Opinion 1/2010***).

12 *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth) sch4 s2A (***Privacy Amendment***).

13 Australian Privacy Principles 3, 5, 10.1.

14 APP 6, 7, 11, 12 and 13.

15 APPs 1.3-1.6.

16 APP 4.

17 APP 8.

18 APP 9.

19 APP 2.

20 APP 1.2.

21 *Opinion 1/2010,* above n11, 29.

22 Email correspondence from Basil Newnham, Symantec Corporate Counsel, to Kanin Lwin, 26 November 2013.

23 Ibid.

24 APP Guidelines, Ch B, 'Use'.

25 APP Guidelines, 'Preface'.

26 IPP Guidelines, Ch 8, 'Relationship between use and disclosure'.

27 *Opinion 1/2010,* above n11, 29.

privacy obligations outside their capability to comply. For example, APP 12 requires entities holding personal information to grant access to that data upon request. Even if cloud providers can be said to hold data that resides on their servers, insofar as entities 'hold' personal information under their possession or control,[28] they often lack the capacity to provide access. Where a client has chosen to secure their data through a method like multi-blind key encryption, wherein they essentially retain both the encryption and de-encryption keys,[29] a provider would depend entirely on the customer's assistance to comply with APP 12. Likewise, APP 6 obliges entities to use personal information only for the purpose(s) for which it was collected. However, cloud providers who process data which the client collects are unlikely to know this purpose or share the same purpose as the original collector.

Regulatory

Any reading of the APPs which reduces the number of entities to whom they apply might be said to favour practicality at too great a cost to privacy. However, making providers accountable for obligations with which they cannot feasibly comply does not necessarily stimulate better compliance with the APPs. Instead, expanding the number of entities that have privacy obligations may unnecessarily dilute privacy responsibility[30] and reduce the cost and burden of compliance for cloud computing customers who are both the controller and collector, given liability may now be shared with the provider.

Any reading of the APPs which reduces the number of entities to whom they apply might be said to favour practicality at too great a cost to privacy

Commercial

A favourable and more targeted application of the APPs to cloud computing is also more consistent with a drive to develop Australia as a consumer and vendor of digital services through a mixture of 'conducive' regulations and 'digital infrastructure' like the NBN[31]. In particular, interpreting the APPs in a manner that avoids fragmenting privacy responsibility would allay consumer concerns and permit Australian businesses to expand their use of outsourcing arrangements like cloud computing. Furthermore, more realistic distinctions in the application of privacy obligations would enhance Australia's attractiveness as a regional data-hub and potentially, be more consistent with the approach taken in other jurisdictions including the EU[32] whose privacy regime recognises the functional differences between data processing participants.[33].

Preferred approach

Collectors & controllers

As described above, there is a contextual impetus for interpreting the APPs in a way that acknowledges the different roles various entities play when processing data. One possibility is to recognise that several APPs distinguish between (i) controllers and processors and (ii) collectors and non-collectors, given concepts of 'control' or 'collection' underpin most APPs.

Many obligations in the APPs apply only to controllers or collectors. As a result, processors who are not involved in data collection are answerable for just APPs 1.2 and 11.1 (summarised by the table below) which do not require collection or control. Controllers remain different from collectors given processors can collect personal information on a controller's behalf.[34]

APP	Focus	Lifecycle stage	Appropriate entity
1.2	Compliance procedures	Entire	All
11.1	Security	Handling	
1.3-1.6	Privacy Policies	Collection	Collector
2	Anonymity/ pseudonymity	Collection	
3	Solicited personal information	Collection	
5	Notification of collection	Collection	
9.1	Adoption of government related identifiers	Collection	
10.1	Quality of personal information collected	Collection	
4	Unsolicited personal information	Collection/ Destruction	Controller
6	Use or disclosure	Handling	
7	Marketing	Handling	
8	Cross-border disclosures	Handling	
9.2	Use or disclosure of government-related identifiers	Handling	
10.2	Quality of personal information used or disclosed	Handling	
11.2	Destruction/ de-identification	Destruction	
12	Access	Handling	
13	Correction	Handling	

Rationale

Although this approach adds a collector/non-collector classification to the controller/processor distinction of other privacy regimes, it still balances, more effectively, the economic and privacy implications of the growth in data traffic. A regulatory focus on 'collectors' and 'controllers' enables individuals to exercise their privacy rights against those entities and thereby retain some control over their personal information throughout the lifecycle of processing. This approach of allocating the bulk of privacy obligations according to whether entities 'collect' or 'control' personal information also takes into account the functional differences between data processing participants and so promotes privacy protection without inhibiting outsourcing arrangements like cloud computing.

Cloud providers, in the many situations where they neither collect nor control personal information, would not need to comply with unfeasible obligations like granting access to information outside their control.[35] Instead, they would be exposed only to APPs 1.2 and

28 *Privacy Amendment* sch 1 s24.

29 Symantec Corporation, 'Patent for Systems and Methods for Secure Third-Party Data Storage' (26 September 2013) http://www.faqs.org/patents/app/20130254558

30 *Opinion 1/2010,* above n11, 29.

31 Department of Broadband, Communications and the Digital Economy, Australia's Digital Economy: Future Directions, 2009, 8.

32 Australian Law Reform Commission, *Review of Australian Privacy Law,* Discussion Paper 72 vol 1, 850-854.

33 *Opinion 1/2010,* above n11, 4.

34 *Opinion 1/2010,* above n11, 27.

11.1, obligations providers *can* and *should* comply with at all times. APP 1.2 simply requires that organisations have procedures in place to comply with the relevant APPs. Whilst APP 11.1 obliges entities to take such steps as are reasonable in the circumstances to protect personal information they hold from risks such as 'misuse' and 'unauthorised disclosure', providers need not control or collect data to be able to comply with this obligation.

By virtue of partly or wholly managing the underlying IT infrastructure for an organisation, cloud providers have considerable influence over the protection of personal information within their environment, irrespective of whether they control data collection and handling. Even under an 'Infrastructure-as-a-Service' arrangement, where providers manage only the physical IT resources, providers still have a responsibility to ensure their hardware is not misused to compromise a client's environment: one customer, for example, could run malicious code from the 'cloud' leveraging the solution's considerable physical resources to intensify their attack against other customers.

Controller/processor

The idea of control appears in many APPs either through the proxies of 'use' and 'disclosure' or because there is an assumption that the type of entity to which that particular APP applies has a capacity to deal with personal information that only a controller would have.

- **Use or disclosure – APPs 6-8, 9.2, 10.2 and 11.2.** APPs which incorporate 'use' and/or 'disclosure' of personal information into their scope can only apply if the entity has control over data. APPs 6, 7, 8, 9.2 and 10.2 regulate how an entity may 'use' and/or 'disclose' personal information. APP 11.2 requires entities to destroy/de-identify personal information they can no longer use or disclose. Although 'use' and 'disclosure' are not defined,[36] the Guidelines state that information is 'disclosed' where an entity releases it from its 'effective control'[37] and 'used' if the entity maintains control.[38] This is consistent with the earlier NPP guidelines[39] and mirrors the previous IPP guidelines wherein, for example, disclosure is regarded as a release of effective control.[40]
- **Capacity to decide which data to process – APP 4.** APP 4 obliges entities to decide either to destroy/de-identify or 'collect' unsolicited personal information, depending on whether it could have been legitimately collected. The decision is ultimately one about which data to process (i.e. is it to be collected and processed or destroyed/de-identified), a determination only the controller can make.[41] Consequently, APP 4 should normally only concern those entities acting as controllers.
- **Capacity to grant access – APP 12.** Likewise, the requirement in APP 12 that individuals generally be given access to their personal information implies that an entity has the capacity to grant such access, an ability usually regarded as an exclusive power of controllers.[42]
- **Level of control – APP 13.** APP 13 provides that entities must, under certain circumstances, correct the personal information they hold. The Explanatory Memorandum notes that APP 13 is designed to normally force entities into assessing the quality of personal information they hold 'at the time of use or disclosure',[43] indicating that APP 13 is primarily directed at controllers.

Collector/non-collector

- **APPs 3, 5 and 10.1.** Some of the APPs bear little relevance for non-collectors. For instance, APP 3 restricts when entities can collect personal information whilst APPs 5 and 10.1 regulate how collection can occur. Other provisions like APPs 1.3 to 1.6, 2 and 9.1 presume the entity is a collector notwithstanding language which might read as applying to non-collectors as well.
- **APPs 1.3 to 1.6.** These APPs require entities to develop and disseminate privacy policies according to specific standards. Although 'APP entity' encompasses collectors and non-collectors, APP 1.4 states that privacy policies must declare what personal information that entity 'collects and holds' and so makes little sense for non-collectors.
- **APP 2.** This principle grants individuals a right to anonymity or pseudonymity when 'dealing' with entities. As such a right ensures entities seek only the minimum amount of personal information necessary, APP 2 potentially applies to two stages in the lifecycle of information processing: (i) when an entity collects personal information from the data subject or (ii) holds that information beyond what is necessary.[44] However, it is unlikely APP 2 extends to encompass non-collectors. APP 11.2 already deals with the de-identification of personal information which has ceased to be relevant to the purpose for which such data could be legitimately used or disclosed. Furthermore, the Explanatory Memorandum rationalises APP 2 primarily on the basis 'the privacy of individuals will be enhanced if their personal information is not *collected* unnecessarily'.[45]
- **APP 9.1.** APP 9.1 generally prohibits organisations from 'adopting' government related identifiers. Given the Guidelines define adoption in terms of the collection and organisation of personal information[46], this prohibition seems geared toward collectors.

Conclusion

Opportunities for vast movements of data offer considerable economic benefits but pose serious privacy concerns, in particular the growing incentive and ability to harvest this traffic for valuable private data. To accommodate this tension without inhibiting outsourcing arrangements like cloud computing, certain privacy regimes take into account the functional differences between data processing participants, usually in terms of control. The APPs strike a similar balance between privacy and practicality, albeit by allocating many obligations to 'controllers' or 'collectors'. As the market and value proposition for cloud services grows, these classifications offer a means of interpreting the APPs in a manner which avoids burdening providers (where they act as processors and non-collectors) with unfeasible obligations that unnecessarily fragment privacy responsibility. Furthermore, the focus on controllers and collectors also better aligns Australia's regulations with the emerging 'digital economy' both in terms of capturing a slice of the growing cloud services market and encouraging Australian businesses to drive productivity gains by embracing the 'cloud'.

Kanin Lwin is a graduate at Ashurst Australia and was a finalist in the 2014 CAMLA Young Lawyers Essay Competition for an earlier version of this essay.

35 APP 12.
36 *Privacy Act 1988* (Cth) s6.
37 APP Guidelines, Ch B, 'Disclosure'.
38 APP Guidelines, Ch B, 'Use'.
39 NPP Guidelines, 35-42, 'Use and disclosure'.
40 IPP Guidelines, Ch 8, 'The meaning of use and disclosure of information'.
41 *Opinion 1/2010,* above n11, 16.
42 *Opinion 1/2010,* above n11, 17.
43 Explanatory Memorandum, 88.
44 Anneliese Roos, 'Core Principles of Data Protection Law' (2006) 39 *Competition and International Law Journal,* 113-114.
45 *Explanatory Memorandum* 74.
46 APP Guidelines, Ch 9, 'Adoption'.

California Pioneers New Law to Protect Young People from Online Privacy and Advertising Abuses

Dr. Alana Maurushat, David Vaile and Carson Au examine recent reforms to the law in California regarding the privacy of minors and consider whether Australia should enact similar provisions.

Introduction

Governments face a number of issues with youth, online technologies and privacy. Children are sending one another provocative and sexualized self-images ("sexy selfies") and violent content via SMS, Facebook, Snapchat and other social networks, without realising the potential consequences. Companies are collecting vast amounts of data from minors without adequate consent. Advertisers are using social network sites to market in a fashion not otherwise permitted in the offline world.

While many jurisdictions have attempted to tackle these privacy issues using educational campaigns and longstanding privacy principles, other jurisdictions such as California have proposed new online privacy bills dedicated to children. This article examines two recently proposed California privacy bills and discusses whether Australia should consider enacting similar provisions.

Companies are collecting vast amounts of data from minors without adequate consent

California Bills

Two Californian Senate Bills were introduced in 2013 concerning, children and digital privacy: Senate Bill 501[1] (***Social Networking Privacy Act*** *or* ***SB 501***) and Senate Bill 568[2] (***Privacy Rights for California Minors in the Digital World*** *or* ***SB 568***).

The Social Networking Privacy Act (SB 501)

The California Senate has passed SB 501, but it still remains in the Assembly as of February 2014. SB 501 applies to both adults and minors (those under 18 years of age) residing in California. It requires 'a social networking Internet Web site to remove the personal identifying information of a registered user that is accessible online'[3] within 96 hours upon request of the user.[4] A registered user means any persons who have created an account for the purpose of accessing the social networking site.[5] However, for users who are minors, the site is also required to remove the content upon the request of the parent or legal guardian of the minor.[6]

The obligation to remove personal information is imposed on social networking Internet Web sites, which are expressly defined as 'service[s] that allow an individual to construct a public or partly public profile within a bounded system, articulate a list of other users with whom the individual shares a connection, and view and traverse his or her list of connections and those made by others in the system'.[7] Since the word 'connection' is not defined, the scope is broad and is not limited to services such as Facebook and Twitter. For example, it is arguable that YouTube, a website primarily for videos, falls within the scope of this definition because it enables users to connect to other users by subscribing or commenting on another user's video. The user can additionally click on the profiles of other users and browse through the connections that the user has made (e.g. the videos that he or she has commented on). An e-commerce site that enables customers to review products and comment on other customer's reviews and browse other customer's profiles and previous product reviews, would similarly fall within this scope.

The bounds of 'personal identifying information' are expressly limited to a person's:

street address;
telephone number;
driver's license number;
state identification card number;
social security number;
employee identification number;
mother's maiden name;
demand deposit account number;
savings account number; or
credit card number.

There are clearly a range of data items potentially useful for effectively identifying individuals which are not covered, including inter alia other forms of financial system identifiers, other account names, identifiers including nicknames, and technical identifiers such as those broadcast by a child's mobile phone or computer or inserted by way of tracking technologies onto their device.

SB 501 imposes a civil penalty of no more than US$10,000, for each wilful and knowing violation.[8]

The primary criticism of SB 501 is that it burdens the free expression of minors. Parents of children would be able to request the removal of any social networking posts of their children.[9] Additionally, because of the inherent difficulty of verifying identity on the

1 Sen. Bill No. 501 (California) http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB501
2 Sen. Bill No. 568 (California) http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB568
3 Sen. Bill No. 501 § 60(a)
4 Sen. Bill No. 501 § 62(a)
5 Sen. Bill No. 501 § 62(c)
6 Sen. Bill No. 501 § 62(a)
7 Sen. Bill No. 501 § 62(c)
8 Sen. Bill No. 501 § 65
9 Llanso, E 2013, 'Comments on SB 501: The Social Networking Privacy Act and SB 568, Regarding Privacy Rights for California Minors in the Digital World', *Center for Democracy & Technology,* viewed 28 November 2013, <https://www.cdt.org/files/pdfs/CDT-Testimony-SB501-SB568.pdf>

Internet, SB 501 may be subject to abuse.[10] SB 501 may also impose a significant burden on operators, which may lead to operators banning minors from using their products and services.

Privacy Rights for California Minors in the Digital World (SB 568)

SB 568 was signed into Californian law on 23 September 2013 and will take effect on 1 January 2015 as *California Business and Professions Code* § 22580-82. SB 568 imposes obligations with respect to advertising and content removal.[11] ReedSmith has published a useful flowchart explaining the application of SB 568,[12] which is summarised below.

The content removal obligations imposed by SB 568 apply to operators of Internet Web sites, online services, online applications or mobile applications 'directed to minors'[13] where the operator has actual knowledge that a minor is using its services. The phrase 'directed to minors' is defined as having 'the purpose of reaching an audience that is predominantly comprised of minors, and is not intended for a more general audience comprised of adults'.[14] This definition is vague. For instance, cartoon mobile games such as Angry Birds may arguably have been intended for audience that is predominantly minors. However, since the game has become popular with adults, it is also arguable that it is intended for a more general audience. The 'actual knowledge' requirement does not require operators to inquire about the user's age.[15] Subsequently, operators can avoid liability by not collecting age information or by banning minors upon obtaining such information.

Such operators must notify registered users who are minors of their right to request and to obtain removal of content posted on the operator's Internet site, service or application by the minor.[16] Clear instructions on this procedure must also be provided.[17]

Nevertheless, there are exceptions where the operator is not obliged to remove the content upon request. Notably, if the content at issue is posted by a third party, even if the content was a re-publication or a re-post of the aggrieved minor's initial post, the operator is not obliged to remove the content.[18] This will also be the case where the operator de-identifies the content such that the minor cannot be individually identified or if the minor has received compensation or consideration for the content.[19] Furthermore, an operator is deemed to have complied with SB 568 if the original posting was made invisible to the public, even if the content remains visible because it has been copied or re-posted by a third party.[20]

These exceptions may render the practical application of SB 568 ineffective, especially given that in many cases, the more embarrassing the post, the more likely it is to be shared by third-parties.[21]

SB 568 imposes advertising restrictions on operators of Internet Web sites. For example, if an operator of an Internet Web site, online service, online application or mobile application is 'directed to minors', then under SB 568 they will be prohibited from marketing or advertising goods and services listed in § 22581(i).[22] Examples include firearms and alcoholic beverages. The operator is not required to have actual knowledge that minors are users.

Alternatively, a similar operator who has actual knowledge of minors using its site, service or application (regardless of whether it is 'directed to minors') is prohibited from marketing or advertising the § 22581(i) goods and services to the minor if the marketing or advertising is based upon information specific to that minor.[23]

While many jurisdictions have attempted to tackle these privacy issues using educational campaigns and longstanding privacy principles, other jurisdictions such as California have proposed new online privacy bills dedicated to children

Finally, if a similar operator has actual knowledge of minors using its site, service or application, or has actual knowledge that the site, service or application is 'directed at minors', the operator shall not knowingly (or allow a third party) 'use, disclose, compile ... the personal information of a minor with actual knowledge' that it is for the purposes of marketing or advertising the § 22581(i) goods and services to that minor.[24]

SB 568 has been criticized on a number of grounds including vagueness of law, its ineffectiveness, its over-ambition and its potential loopholes. Eric Goldman, a Professor of Law at Santa Clara University School of Law, highlighted several uncertainties,[25] which are set out below.

---

10 Above, n8 at 1.

11 Goldman, E 2013, 'California's Latest Effort To 'Protect Kids Online' Is Misguided and Unconstitutional', *Forbes - Eric Goldman – Tertium Quid blog, 24* September, viewed 28 November 2013, <http://www.forbes.com/sites/ericgoldman/2013/09/30/californias-latest-effort-to-protect-kids-online-is-misguided-and-unconstitutional/>

12 ReedSmith 2013, *Reference Guide to SB 568 – Internet Privacy For California Minors*, ReedSmith, viewed 28 November 2013, <http://www.globalregulatoryenforcementlawblog.com/uploads/file/Internet%20Privacy%20for%20CA%20Minors%20-%20Reference%20Diagram_phcho.pdf>

13 Sen. Bill No. 568 § 22581(a)

14 Sen. Bill No. 568 § 22580(e)

15 Sen. Bill No. 568 § 22581(e)

16 Sen. Bill No. 568 § 22581(a)

17 Sen. Bill No. 568 § 22581(a)

18 Sen. Bill No. 568 § 22581(b)

19 Sen. Bill No. 568 § 22581(b)

20 Sen. Bill No. 568 § 22580(d)

21 Karohonik, T 2013, 'Why California's new online privacy bill will cause more problems than it solves', *New Media Rights*, 25 September, viewed 28 November 2013, <http://www.newmediarights.org/that%E2%80%99s_great_idea%E2%80%A6_pity_it_won%E2%80%99t_work_look_why_california%E2%80%99s_new_online_privacy_bill_will_cause_more>

22 Sen. Bill No. 568 § 22580(a)

23 Sen. Bill No. 568 § 22580(b)

24 Sen. Bill No. 568 § 22580(c)

25 Goldman, E 2013, 'California's New 'Online Eraser' Law Should be Erased', Forbes - *Eric Goldman – Tertium Quid blog*, 24 September, viewed 28 November 2013, <http://www.forbes.com/sites/ericgoldman/2013/09/24/californias-new-online-eraser-law-should-be-erased/>

First, for SB 568 to apply to an operator, the operator's website or app must be 'directed' to minors. It is difficult to distinguish between content aimed at young adults, and content aimed at 17 year olds. Many websites such as Instagram, or apps such as Angry Birds are popular with both minors and young adults. [26]

Second, SB 568 provides that the minor has the right of removal, but does not define when the minor can exercise the removal right. It is unclear whether an adult will have the right of removal for content initially posted when they were a minor. If not, the law would then require minors to make arguably mature and adult decisions (that is, on what content they wish to keep in the public for the rest of their lives) whilst being still minors.

Third, the advertising restrictions do not define 'personal information,' nor does it explain what constitutes an 'advertising service'.

SB 568 only provides the right of removal of the initial post by the user. If the post is copied to another site, or shared by another user, no right of removal will exist. This is particularly problematic as the more embarrassing a post or a photo is, the more likely that it is to be shared. [27]

SB 568 has been criticized on a number of grounds including vagueness of law, its ineffectiveness, its over-ambition and its potential loopholes

SB 568 only imposes burdens on operators with actual knowledge of minors using its products and services. By not collecting age information at all, websites are able to escape the operation of this law. [28]Further, SB 568 does not state that the content removal mechanism has to be automated. It only requires that it is available. By making the mechanism sufficiently difficult to use, slow or onerous (e.g. by requiring users to request removal via physical mail), the operator may be able to significantly reduce such requests. [29]

While there are plenty of criticisms of both SB 501 and SB 568, there is merit to the argument that something needs to be done to safeguard minors' privacy online. It is a useful contribution to regulation addressing online harms suffered most acutely by young people.

The Australian Framework

Privacy issues relating to youth and social networking sites are not regulated separately in Australia but are instead included within the general scope of privacy law under the Australia Privacy Principles (***APPs***), which take effect on 12 March 2014. These ten principles are:

APP 1: open and transparent management of personal information
APP 2: anonymity and pseudonymity
APP 3: collection of solicited personal information
APP 4: dealing with unsolicited personal information
APP 5: notification of the collection of personal information
APP 6: use or disclosure of personal information
APP 7: direct marketing
APP 8: cross-border disclosure of personal information
APP 9: adoption, use or disclosure of government related identifiers
APP 10: quality of personal information
APP 11: security of personal information
APP 12: access to personal information
APP 13: correction of personal information

There is no general common law or statutory right to privacy in Australia, although the latter is under consideration by the Australian Law Reform Commission. This means that if a young person falls through this regime there is often little in the way of a remedy.

SB 501 and SB 568 offer a list of 'personal identifying information' which include a person's street address, telephone number, and so forth, consistent with other US usage. Australian law, in keeping with other OECD practice, uses a broader definition of 'personal information.' Under section 6 of the *Privacy Act 1988* (Cth) (the ***Privacy Act***), 'personal information' means information or an opinion about an identified individual, or an individual who is reasonably identifiable: (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in a material form or not.

Information from which identity "can reasonably be ascertained" potentially extends quite broadly, focusing on the function of identification (which can change with developments in business process or data handling, such as the Big Data capabilities for re-identification of previously de-identified or anonymised records) rather than a fixed list of identifiers which represent only a subset of data items useful for identification purposes.

However, section 16 of the Privacy Act exempts personal, family or household affairs, consistent with the Act's original focus on business and government records:

> Nothing in the Australian Privacy Principles applies to: (a) the collection, holding, use, disclosure or transfer of personal information by an individual; or (b) personal information held by an individual; only for the purposes of, or in connection with, his or her personal, family or household affairs.

The commissioner rarely makes determinations, so there is in effect no body of law about interpretation of such provisions, but it is clearly open to treat most communications between individuals about their "personal affairs" as in effect outside the scope of the Privacy Act. Most of the relevant actions are thus undertaken by people outside the ambit of the Privacy Act, or potentially within it but outside the jurisdiction.

In the context of online social networking sites (most of which are operated or owned by businesses incorporated in America using American law, as per the applicable in the terms and conditions), but in some cases potentially subject to Australian consumer protection law), and in the absence of a general enforceable right to privacy in Australia, the Privacy Act plays a small role. If for example, a minor or a minor's guardian wished to have personal information removed from a minor's Facebook account, they could request that Facebook (for example) remove the content. Facebook has no legal obligation absent a court order to remove any content. The decision lies with the online social network. While the Australian privacy framework is available to the minor, it would require a formal complaint to be made to the Privacy Commissioner, who may look into the issue, decide to investigate and then render a decision within two months to ten years. During this process, the Commissioner may meet with the online social network provider and advise as to how to best change practices to prevent future privacy breaches, if indeed a privacy breach was even present. This framework, given the low rate of determinations made over the years and the slow response time[30] compared to the high volume of rapidly shared unwanted publications about young people, is largely irrelevant for many of the real problems with personal identification information, social network sites and minors (and adults as well).

---

26 Above, n19 at 5.

27 Above, n19.

28 Above, n19.

29 Above, n19.

Advertising and marketing is regulated in Australia. Each State has its own codes and regulations affecting advertisers and marketers, and the *Competition and Consumer Act 2010* (Cth) (embodying the Australian Consumer Law) likewise applies throughout Australia. Australian consumer law covers some main areas related to advertising including: misleading and deceptive conduct; false or misleading representations; unconscionable conduct; representations about country of original, and information standards. These statutes, however, do not expressly contain any provisions specific to marketing and advertising to minors, and the extent to which they apply to online services remains ambiguous.

It is unclear whether an adult will have the right of removal for content initially posted when they were a minor

The area is additionally self-regulated by the Advertising Standards Bureau who 'administers a national system of advertising self-regulation through the Advertising Standards Board and the Advertising Claims Board.'[31] Online marketing and advertising to minors using social network sites has two distinct advantages. First, there are no laws or regulations specific to minors. Second, as most online social network sites are American, Australian law has little to no extra-territorial effect (though the effect of the Australian Consumer Law can be seen in Australian-specific clauses, drawing attention to non-excludable protections, in licences from offshore online entities like Adobe and Apple). While a party could complain to the appropriate regulatory authority such as the ACCC, the chances of obtaining an effective remedy are slim to none, unless there is an Australian presence.

Conclusion

California has been a pioneer of modern privacy law with the first introduction of mandatory data breach notification legislation, a very powerful spam law in 2003 (sadly over-ridden by the spam friendly federal CAN-SPAM Act of 2003), and now reforms addressing privacy, online technologies and minors. There are clear issues here which require action but sometimes the best approach is to wait and see. If California successfully enacts SB 501 and SB 568, there will be ample evidence within a few years of their operation as to their effectiveness and problematic components. If enough jurisdictions begin to legislate in the area, large companies such as Facebook and WhatsApp may begin to self-regulate so that their internal practice will reflect stricter more protective practice as required under the law. Some corporations may also choose to comply with the most stringent privacy law from one significant jurisdiction (eg. Europe) as opposed to having different technical platforms and marketing practices in every jurisdiction that they operate. In the aftermath of recent concerns over data sovereignty, this effect may grow stronger in the near term.

Dr Alana Maurushat, David Vaile and Carson Au are members of the Cyberspace Law and Policy Community, Faculty of Law, at the University of New South Wales.

---

30 Connolly, C and Vaile, D. Communications privacy complaints: in search of the right path, Cyberspace Law and Policy Centre, UNSW, 14 September 2010 <http://cyberlawcentre/org/privacy/ACCAN_Complaints_Report/report.pdf> .

31 Advertising Standards Bureau, http://www.adstandards.com.au/aboutus/aboutselfregulation.

CAMLA's Young Lawyers Event 2014 - Another 'Sell Out'!

CAMLA's second event for young and junior lawyers was held on 11 February 2014 at Baker & McKenzie in Sydney and was well oversubscribed and attended!

Organised by CAMLA's Young Lawyers Committee, the evening took a light-hearted panel format comprising Toby Ryston-Pratt (Deputy Chief Legal Counsel, NBN Co), John Corker (Visiting Fellow, UNSW), Andrew Stewart (Partner, Baker & McKenzie), and Sandy Dawson (Barrister, Banco Chambers) and was moderated by Ryan Grant (Senior Associate, Baker & McKenzie). The panellists provided the audience with fascinating insights into their career journeys so far and advice to young lawyers as to where their law degrees and experience may take them.

The event also included the presentation of awards for the prize-winners in the CAMLA essay competition. Prizes were awarded to Jarrod Bayliss-McCulloch of Baker & McKenzie for his essay entitled "Does Australia need a 'right to be forgotten' ?", Kanin Lwin of The University of Sydney for his essay entitled "Australia's Privacy Principles And Cloud Computing: Another Way" and to Michael Douglas of The University of Western Australia for his essay entitled "Intervention of Media Organisations in First Instance Proceedings: A Matter of Natural Justice". The essays were judged by representatives of private practice, industry and academia. Awards were announced and presented by CAMLA President, Page Henty.

By all reports the panel presentation, synopses of prize winning essays (and of course plentiful refreshments) we enjoyed by all, with many looking forward to the next event. Particular thanks must go to each of the panellists for their time, insights and advice, and to Baker & McKenzie for hosting the event.

Stay in touch with CAMLA via our website (www.camla.org.au) and LinkedIn page for news on upcoming CAMLA events, the bulletin and membership information.

Communications & Media Law Association Incorporated

The Communications and Media Law Association (**CAMLA**) brings together a wide range of people interested in law and policy relating to communications and the media. CAMLA includes lawyers, journalists, broadcasters, members of the telecommunications industry, politicians, publishers, academics and public servants.

Issues of interest to CAMLA members include:

- defamation
- broadcasting
- copyright
- advertising
- information technology
- freedom of information
- contempt
- privacy
- censorship
- film law
- telecommunications
- the Internet & on-line services

In order to debate and discuss these issues CAMLA organises a range of seminars and lunches featuring speakers prominent in communications and media law policy.

Speakers have included Ministers, Attorneys-General, members and staff of communications regulatory authorities, senior public servants, executives in the communications industry, lawyers specialising in media and communications law, and overseas experts.

CAMLA provides a useful way to establish informal contacts with other people working in the business of communications and media. It is strongly independent, and includes people with diverse political and professional connections. To join CAMLA, or to subscribe to the Communications Law Bulletin, complete the form below and forward it to CAMLA.

Disclaimer

The Communications Law Bulletin is the journal of the Communications and Media Law Association (**CAMLA**) which is an independent organisation which acts as a forum for debate and discussion and welcomes the widest range of views. The views expressed in the Communications Law Bulletin and at CAMLA functions are personal views of the respective authors or speakers. They are not intended to be relied upon as, or to take the place of, legal advice.

Contributions & Comments

Contibutions and Comments are sought from the members and non-members of CAMLA, including features, articles, and case notes. Suggestions and comments on the content and format of the Communications Law Bulletin are also welcomed.

Contributions in hard copy and electronic format and comments should be forwarded to the editors of the Communications Law Bulletin at editor@camla.org.au or to

Valeska Bloch or Victoria Wark
C/- Allens
Deutsche Bank Place
Corner Hunter & Philip Streets
SYDNEY NSW 2000

Tel: +612 9230 4000
Fax: +612 9230 5333

CAMLA contact details:

Email: camla@tpg.com.au
Phone: 02 9399 5595
Mail: PO Box 237,
KINGSFORD NSW 2032

CAMLA Website

Visit the CAMLA website at www.camla.org.au for information about CAMLA, CAMLA seminars and events, competitions and the Communications Law Bulletin.

Application for Membership

To: The Secretary, camla@tpg.com.au or CAMLA, Box 237, KINGSFORD NSW 2032
Phone: 02 9399 5595

Name:.....

Address: .....

Telephone: .....Fax: .....Email: .....

Principal areas of interest: .....

.....

I hereby apply for the category of membership ticked below, which includes a Communications Law Bulletin subscription, and enclose a cheque in favour of CAMLA for the annual fee indicated:

☐ I Ordinary membership $130.00 (includes GST)

☐ Student membership $45.00 (includes GST)
(please provide photocopy of student card - fulltime undergraduate students only)

☐ Corporate membership $525.00 (includes GST)
(list names of individuals, maximum of 5)

☐ Subscription without membership $150.00 (includes GST)
(library subscribers may obtain extra copies for $10.00 each + GST and handling)