THE GLOBAL CHANGING PRIVACY LANDSCAPE

BACKGROUND PAPER

PRIVACY AWARENESS WEEK 2012

INFORMATION INTEGRITY SOLUTIONS PTY LTD

TABLE OF CONTENTS

1 EXECUTIVE SUMMARY

Information Integrity Solutions P/L delivered the first McAfee Background Paper in November 2010, and since that time privacy has moved from a mainstream topic to one that carries heightened concern and significance. The purpose of this paper is to present an overview of the global privacy landscape since November 2010 up to this point, from the key regulatory developments at home and abroad to the upcoming privacy challenges raised by new technologies.

Since 2010, there has been acceleration in the type and quantity of information use. Companies are making headlines both for their technological achievements as well as their frequent missteps over privacy and information handling. There has been a stream of highly publicised data breaches, from global giants like Epsilon and Sony to local incidents involving Vodafone and Telstra. In this context, privacy has taken a prominent position in the minds of individuals, businesses and regulators.

On the regulatory front, there has been mixed progress in the Asia-Pacific region:

- 2011 saw encouraging developments in Australia, with the release of the Exposure Draft provisions of the Australian Privacy Principles and credit reporting. However, since the release of the Senate Committee's accompanying reports, the pace has slowed, with the chance that we may see some amending legislation introduced to Parliament before 30 June 2012.

- In contrast, the past 18 months have been a busy period in many Asian countries. Some jurisdictions such as Malaysia and the Philippines have adopted data protection law for the first time, while others such as Singapore are progressing rapidly towards a draft proposal.

- After more than five years in development, APEC's system for cross-border privacy protection and information sharing has been finalised.

2012 also saw the two major players — the European Union and the United States — outline new, albeit diverging proposals for privacy reform. The EU released a Draft Regulation on the protection of individuals and their personal data. The Regulation is sweeping in scope, with important provisions relating to data breach notification, penalties and the right to be forgotten. Meanwhile, the American focus is on the protection of consumers in the online environment. Rather than a top-down approach, officials will collaborate with industry to adopt self-regulatory codes. Now we can only take a wait-and-see approach as each jurisdiction grapples with the twin challenges of implementation and enforcement.

Today we are facing new privacy challenges through the convergence of technological advancement, increasing computing power and the proliferation of mobile devices:

- Do Not Track —There is a huge market devoted to tracking individuals' online activities and selling that information. The advertising industry is responding to privacy concerns by pledging to implement a Do Not Track system, but one that has shortcomings.

- Big Data — Companies combing through voluminous quantities of data can not only exploit them for new purposes, but also piece together personal information.

- Facial recognition — Beyond law enforcement, facial recognition will have growing importance in commercial and social contexts. With so many cameras and photo-sharing capabilities available, the potential for creepy applications abound.
- Location technology — The accuracy of technology combined with the ubiquity of mobile phones will provide plenty of scope for new uses, and abuses, of location information.

For businesses, now is a time of unprecedented opportunity. The availability of outsourcing and cloud computing allows for huge improvements in efficiency and increase in capacity. Big Data and facial recognition and location technology are opening up new avenues and markets. Whether companies are able to access the full potential of these opportunities may well depend on the extent they prove that they can respect the privacy of the personal information that is in their custody.

2 THE CHANGING PRIVACY REGULATORY LANDSCAPE AT HOME AND ABROAD

2.1 AUSTRALIA

Currently privacy reform in Australia is still proceeding at a glacial pace.

The Australian Government is structuring the first stage of amendments to the privacy legislation into four components. The Exposure Draft provisions and report of the Senate Committee are now available for two of them — the Australian Privacy Principles and credit reporting. The other two — relating to protection of health information and strengthening the Privacy Commissioner's powers — are yet to be released. It is expected that a draft bill containing the APPs and credit reporting will be introduced in either the Budget or Winter 2012 sittings of Parliament.

The second stage of the Government's response will address the remaining recommendations in the ALRC report, including the clarification or removal of exemptions, serious data breach notification and a statutory cause of action for serious invasion of privacy. In September 2011, the Government released an Issues Paper titled "A Commonwealth Statutory Cause of Action for Serious Invasion of Privacy" and called for submissions in response.[1] The government has not yet released its response to the submissions received. There is also no word as to when the second stage responses will be released, raising the prospect that comprehensive privacy reform will not be complete for some time yet.

The Australian Government is also seeking submissions to develop a Cyber White Paper that will outline a strategy for how government, businesses and citizens can optimally engage online. One area of particular interest is the policy proposal for a national trusted identities framework, which comes in the wake of governments around the world tackling the issue of identity management and trust in the digital environment.

2.1.1 SENATE COMMITTEE REPORT ON AUSTRALIAN PRIVACY PRINCIPLES

A key recommendation of the 2008 Australian Law Reform Commission's report into privacy reform was the unification of the existing privacy principles — the Information Privacy Principles (IPPs) for the Commonwealth public sector and the National Privacy Principles (NPPs) for the private sector. As part of its reform package the Australian Government in June 2010 released the Exposure Draft of the new Australian Privacy Principles (APPs) which will form the cornerstone of the new Privacy Act. The Senate Finance and Public Administration Legislation Committee ('the Committee') delivered the corresponding report in June 2011.[2]

[1] Department of the Prime Minister and Cabinet, *Issues Paper – A Commonwealth Statutory Cause of Action for Serious Invasion of Privacy*: <http://www.dpmc.gov.au/privacy/causeofaction/docs/issues%20paper_cth_stat_cause_action_serious_invasion_privacy.pdf> (September 2011).

[2] Parliament of Australia, *Senate Committee Report Part 1 – Australian Privacy Principles*: <http://www.aph.gov.au/Parliamentary_Business/Committees/Senate_Committees?url=fapa_ctte/priv_exp_drafts/report_part1/index.htm> (15 June 2011).

2.1.1.1 CLARIFYING THE APPS

The Committee's report noted that the goal of drafting the APPs was to ensure that they are streamlined, framed at a high level and easy to understand. Many submissions were concerned that the draft APPs are overly complex and lack clarity, pointing to its legalistic language, repeated use of long terms and its myriad exceptions and provisions, for example APP 3 (collection) and APP 7 (direct marketing). The committee recommended reassessing the draft principles with a view to improving clarity.

2.1.1.2 'PERSONAL INFORMATION'

The definition of 'personal information' in section 15 of the draft provisions relates to information by which an individual is identified or is reasonably identifiable.[3] Some submissions argued that the new definition potentially expands the current scope of personal information and may lead to increased burdens on those bound by the Privacy Act. However, the expansion is consistent with the direction being taken in both the US and Europe in their recent initiatives to rewrite their respective privacy frameworks.

The committee recommended that the Office of the Australian Information Commissioner (OAIC) develop guidance on the interpretation of 'personal information' as a matter of priority.

2.1.1.3 SMALL BUSINESS EXEMPTION

The Companion Guide to the draft APPs indicates that the small business exemption from the NPPs under the current Privacy Act will be retained. A number of submissions called for the removal of the small business exemption, arguing that the nature of the information, not the size of the organisation, should determine restrictions on what is collected. The committee recognised that the cost of compliance was a significant concern for the small business community. It considered that 'no further comment is required at this stage,'[4] thus implicitly endorsing the view that the exemption should remain.

2.1.1.4 COLLECTION OF PERSONAL INFORMATION

Under APP 3, an entity can only collect personal information which is reasonably necessary for, or directly related to, one or more of the entity's functions or activities. Some submissions were concerned that the addition of 'reasonably' unnecessarily broadens the collection principle and that it focused only on the entity's functions or activities rather than the individual's reasons for disclosing the information. There was also discussion about the 'directly related' requirement, which is drawn from the IPPs and is intended to enable public agencies to collect information in carrying out its functions.

The committee considered APP 3 a 'less than elegant solution' to the drafting of a unified collection principle. It recommended further consideration be given to whether the addition of 'reasonably' in the 'necessary' test weakens the principle. It also recommended that organisations be excluded from the 'directly related to' requirement.

[3] Cf the current definition in the Privacy Act: 'an individual whose identity is apparent, or can reasonably be ascertained' from the relevant information.

[4] Senate Finance and Public Administration Committee, *Exposure Drafts of Australian Privacy Amendment Legislation Part 1 – Australian Privacy Principles*, p 37.

2.1.1.5 CROSS-BORDER DISCLOSURE OF PERSONAL INFORMATION

Perhaps the most important and contentious changes proposed in the Exposure Draft concern the cross-border issue. Under APP 8, an entity disclosing personal information to an overseas recipient must take steps reasonable in the circumstances to ensure that the recipient does not breach the APPs. There are several notable differences with the current regime:

- APP 8 uses the term 'disclosure' rather than 'transfer' (NPP 9) — the emphasis is on whether information is seen, rather than moving across borders. This means that a disclosure will occur when an overseas recipient accesses information, whether or not the personal information that is accessed is stored in Australia or elsewhere.
- APP 8 applies to agencies as well as organisations.
- Section 20 of the Exposure Draft provides that the disclosing entity is *fully accountable* where the overseas recipient engages in an act that would breach the APPs.

Section 20 was introduced to address the current position in which an organisation transferring personal information to an overseas recipient could potentially avoid liability for subsequent breaches of the Privacy Act. The committee noted that the 'reasonable steps' referred to in APP 8 will generally involve contractual arrangements, and called on the OAIC to develop guidance on this matter.

Once in place, the new cross-border rules will have a significant impact on many organisations. With the rise of international commerce, outsourcing and cloud computing, it is likely that at some point organisations will be disclosing personal information to overseas recipients. Many questions surround the application of the accountability provision in section 20, and the committee recommended that the Department of Prime Minister and Cabinet develop explanatory material to address them.

2.1.2 EXPOSURE DRAFT PROVISIONS ON CREDIT REPORTING

The Exposure Draft provisions for Credit Reporting were released in April 2011. The collection, use and disclosure of information for credit reporting purposes is governed by the credit reporting provisions, rather than the APPs. The proposed reform is intended to replace the current credit reporting regime contained in Part IIIA of the Privacy Act.

The impetus for credit reporting reform gained urgency following the 2008 Global Financial Crisis. A key change in the new system is the introduction of five additional data sets available for collection:

- type of each active credit account (for example, mortgage, credit card)
- date of opening each account
- date of closing each account
- account credit limits
- credit repayment history.

The additional data sets result in a more comprehensive reporting regime. This is a significant change as credit providers will be better able assess the creditworthiness of individuals and meet their lending obligations.

The Exposure Draft expands the definition of 'credit provider' beyond banks to include organisations or small business operators that provide credit as a substantial part of its business. The definition also encompasses organisations or small businesses acting as an agent of a credit provider, where they are processing an application for or managing credit.

Division 2 of the Exposure Draft relates to credit reporting agencies. Section 105 channels APP 1, obliging credit reporting agencies to manage credit reporting information in an open and transparent manner. The collection, use and disclosure of such information is limited to the function of a credit reporting business and certain other purposes approved by law. For the first time it is proposed that de-identified information be regulated. Credit reporting agencies may only use (but not disclose) de-identified information when conducting research in relation to the assessment of the creditworthiness of individuals, in compliance with any rules issued by the Information Commissioner.

Division 3 of the Exposure Draft relates to credit providers. Credit providers must notify the individual when collecting personal information that is likely to be disclosed to a credit reporting agency. Credit providers may not use or disclose credit eligibility information about an individual except for consumer credit related purposes, internal management purposes directly related to the provision or management of consumer credit, and certain other purposes approved by law.

For both credit reporting agencies and credit providers, there are provisions relating to information quality, security, access and correction.

2.1.3 SENATE COMMITTEE REPORT ON CREDIT REPORTING

The Senate Committee released its report on the draft amended credit reporting provisions in October 2011.[5] The committee commented that the Exposure Draft implements a more comprehensive credit reporting regime but also noted there were substantial comments in relation to its length and complexity. Its consultations with industry and consumer stakeholders covered five major issues: identity theft; serious credit infringement; hardship flags; complaints handling; and the simplification of definitions. The committee's notable recommendations include:

- A review of the Exposure Drafts to ensure provisions are clear and concise and definitions are consistent.
- In addition to specific requirements for credit reporting, amending the Exposure Draft to incorporate all the relevant requirements of the APPs for credit reporting agencies and credit providers.
- Empowering the Australian Information Commissioner to regularly audit a credit reporting agency and a credit provider selected at random.

[5] Parliament of Australia, *Senate Committee Report Part 2 – Credit Reporting*: <http://www.aph.gov.au/Parliamentary_Business/Committees/Senate_Committees?url=fapa_ctte/priv_exp_drafts/report_part2/index.htm> (6 October 2011).

- Providing a general requirement for notification of destruction of credit reporting information to all recipients of credit reporting information in cases of fraud, not just when an individual makes such a request.

- Inclusion of consumer remedies, similar to those that exist in the National Consumer Credit Protection Act (such as compensation), for consumers adversely affected by contraventions of the credit reporting provisions.

2.1.3.1 CONSUMER REPORTING CODE OF CONDUCT

The Privacy Act empowers the Australian Information Commissioner to issue a binding Code of Conduct in relation to consumer credit records. The current Consumer Reporting Code of Conduct has been in effect since 24 September 1991. A new Code is being developed in consultation with stakeholders and will be an important mechanism in ensuring that credit reporting agencies and credit providers know how to practically apply the credit reporting provisions.

Specific matters referred to the Code of Conduct by the credit reporting provisions include:

- the implementation of open and transparent practices, procedures and systems for managing credit reporting information

- use or disclosure requirements in relation to direct marketing

- manner of giving individuals access to credit reporting information

- additional notification requirements for credit providers when collecting personal information; and

- additional matters when notifying individuals of a refusal of credit.

2.1.4 CYBER WHITE PAPER 2012

In response to the growing opportunities and risks of online engagement, the Australia Government is proposing to release a Cyber White Paper in 2012. The White Paper will be a strategic blueprint, placing the Government's existing initiatives and strategies within an integrated framework as well as fostering partnerships with industry and community groups. Another goal of the White Paper will be to bring cyber issues into the mainstream and to stimulate discussion on how to address risks and challenges.

The public discussion paper[6] set out the following topics to be addressed:

- Digital citizenship in a networked society — what does it mean to be a digital citizen, and what are the implications for traditional notions of privacy, identity and social responsibility?

- Protecting and promoting Australia's digital economy — how can we encourage and facilitate the uptake of digital technologies across the economy, and maintain trust and confidence in e-commerce?

[6] Department of the Prime Minister and Cabinet, *Connecting with Confidence – Public Discussion Paper*: <http://cyberwhitepaper.dpmc.gov.au/sites/default/files/documents/connecting_with_confidence_public_discussion_paper.pdf> (September 2011).

- Security and resilience in the online environment — how do we address cyber threats as well as strengthen the defence of our critical infrastructure?
- International partnerships and internet governance — how can we best develop partnerships with other nations, the private sector and international organisations, as well as engaging meaningfully with the institutions of internet governance?
- Investing in Australia's digital future — what are the ways to invest, educate and build to ensure Australia's future prosperity?

Given the importance of privacy in every facet of online engagement, the Cyber White Paper will no doubt thoroughly address this issue.

2.1.4.1 National trusted identities framework

As part of the Cyber White Paper, the Australian Government is considering including a policy proposal outlining a national trusted identities framework (NTIF). A trusted identities framework allows for the mutual recognition of online credentials by individuals, businesses and government agencies, seeking to authenticate their identity. The NTIF could also address the problem of cyber crime and identity theft as well as facilitate greater online interaction through enhancing confidence and trust.

The following principles were developed following consultation with stakeholders and will inform any future exploration of the viability of an NTIF:

- user control
- respect for privacy
- usability and accessibility
- interoperability across industries and borders
- appropriate risk allocation; and
- supporting innovation and competition while remaining technology-neutral.

Consideration of the NTIF proposal comes in light of international initiatives such as the US National Strategy for Trusted Identities in Cyberspace (NSTIC),[7] the EU's ABC4Trust project[8] and the UK Government's Identity Assurance Programme.[9] This reflects the emergence of identity management as a real issue for governments around the world, as noted in the first McAfee Background Paper delivered by Information Integrity Solutions P/L.

The development of a trusted identities framework would be an important step towards a safer, easier and more efficient way of authenticating identities and interacting online. While the

[7] National Strategy for Trusted Identities in Cyberspace: <http://ww.nist.gov/nstic>.
[8] ABC4Trust EU Project: <https://abc4trust.eu/>.
[9] Government Digital Service, *Posts from the 'ID Assurance' Category*: <http://digital.cabinetoffice.gov.uk/category/id-assurance/>.

Australian Government is likely to be playing a significant role given the complexity of the project, businesses should follow this closely and be attuned to the potential issues.

2.2 NEW ZEALAND

Together with Australia, New Zealand was among the early adopters of privacy law, introducing its Privacy Act in 1993 which was modelled on the 1988 OECD guidelines. In April 2011, the European Commission's data privacy working group issued an Opinion finding its Privacy Act to provide an 'adequate' level of protection for personal data within the meaning of the EU Data Protection Directive.[10] This paves the way for New Zealand to join only 9 other non-European Economic Area jurisdictions to which European personal data may be exported without falling foul of the EU's strict privacy rules.

New Zealand has also recently completed its own comprehensive review of its Privacy Act.[11] Some of the key recommendations in the final report published on 2 August 2011 include:

- More powers for the Privacy Commissioner, including the ability to issue compliance notices and to conduct privacy audits.
- Data breach notification in circumstances where notification may allow the individual to mitigate a significant risk of real harm, or where the breach is serious having regard to its scale and the sensitivity of information.
- Streamlining of the complaints process.
- A new regime to control information-sharing between government agencies.
- Protection against highly offensive and damaging online publication of personal information.

In another move that closely mirrors Australian developments, the New Zealand Privacy Commissioner has made changes to the Credit Reporting Privacy Code. The changes, which took effect on 1 April 2012, enhance the credit reporting industry by allowing the collection of repayment history information. Furthermore, consumers will be able to 'freeze' their credit reports if they are a victim of fraud.

2.3 ASIA

Since Information Integrity Solutions P/L delivered the first McAfee Background Paper there has been a flurry of activity in the Asia-Pacific region, with several jurisdictions adopting privacy and data protection laws for the first time. While the laws have their limitations, there has been a trend towards recognition and enforcement of privacy that is outpacing the law reform effort in Australia.

[10] Article 29 Data Protection Working Party, *Opinion 11/2011 on the Level of Personal Data in New Zealand*: <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp182_en.pdf> (4 April 2011).

[11] Law Commission, *Review of Privacy*: <http://www.lawcom.govt.nz/project/review-privacy?quicktabs_23=report#node-2123>.

The following countries have either introduced or are in the process of introducing privacy law in the last 18 months.[12]

2.3.1 TAIWAN

Taiwan amended its existing 1995 data protection law by enacting the Personal Data Protection Act in May 2010. The Act will apply to both the private and public sector. A data collector will be required to notify the subject to explain the purpose of collection and how the data will be used, as well as obtaining the subject's consent. The use of data must have a justifiable connection with the specified purpose. Notably, the Act has strong penalty provisions, including fines of up to NT$1 million (approx AUS $32,500) or up to five years imprisonment for breaches of the Act. It also allows for the filing of class action law suits. The Act is due to come into force this year.

2.3.2 MALAYSIA

Malaysia enacted (but has not commenced) its Personal Data Protection Act in June 2010, the first of its kind in the country. However, the Act is limited in scope, applying only to personal data in commercial transactions, and not at all to public agencies. The Act has seven principles influenced strongly by the EU Data Protection Directive: Consent; Notice and Choice, Disclosure, Security, Retention, Data Integrity; and Access. Personal data generally may only be used or disclosed for the purposes for which it was obtained, unless the data subject consents. The Act will be enforced once arrangements have been made to establish the Data Protection Commissioner's office.

2.3.3 VIETNAM

Vietnam passed the Law on Protection of Consumer's Rights in November 2010 which took effect on 1 July 2011. Before collecting, using and transferring personal information, businesses must inform the consumer of the purpose of collection, obtain consent to use and are limited in their use to the stated purposes. There are also provisions relating to the secrecy, accuracy and completeness of the information held. Like Malaysia, the Vietnamese law only governs consumers, traders and organisations in the commercial context.

2.3.4 SOUTH KOREA

South Korea passed and promulgated its Personal Data Protection Act in March 2011. The Act regulates all data processors, replacing the old law which only covered the public sector. The collection and use of sensitive data (including universal identifiers) is prohibited unless there is specific consent or authorisation by law. This will have a significant effect on internet activity given the ubiquitous use of resident registration numbers for online registrations. There is a requirement of notification to data subjects of the source of personal data, as well as mandatory data breach notification. On paper the Personal Data Protection Act is one of the best in Asia, and the question now is how it will perform in practice.

2.3.5 SINGAPORE

Following on from a public consultation last year, the Singapore government released its draft Personal Data Protection Bill and a further public consultation paper on 19 March 2012. The Bill is the first of its kind in Singapore and is intended to cover all private sector organisations (but not the public sector), including small businesses. An organisation will be required to obtain an individual's

[12] See Appendix I for table.

consent for the collection, use or disclosure of personal data and the collection must be for reasonable purposes which the organisation discloses. The Bill also has some interesting features:

- No distinction is drawn between personal and sensitive (for example, health) data.
- There are no notification requirements.
- The provisions cover the data of *deceased* individuals up to 10 years from the date of death.
- Importantly for overseas organisations, the law applies if they are engaged in data collection, processing or disclosure within Singapore, even if the organisation may not be physically located in Singapore.

The Singapore government is aiming to introduce the Bill to Parliament by the third quarter of 2012.

2.3.6 The Philippines

On 20 March 2012, the Philippine Senate unanimously approved the Data Privacy Act of 2011, clearing the way for commencement of the first privacy law in the Philippines. The Act is modelled substantially on the EU Data Protection Directive, featuring notice, consent and data breach notification requirements. A National Privacy Commission will be established to implement and enforce regulations. To facilitate the country's sizable outsourcing industry, the law will not apply to personal information collected from residents of foreign jurisdictions in accordance with their laws, which is being processed in the Philippines.

2.3.7 India

India is one major country that is conspicuously without a comprehensive privacy protection regime. Since 2000, the Information Technology Act has required a company possessing, handling or dealing with sensitive personal data to implement reasonable security practices. In April 2011, the Ministry of Communications and Information Technology issued new rules[13] regarding sensitive personal data which includes passwords, financial information, medical records and biometric information. Indian companies are required to notify data subjects of the purpose of collection, to use data only for that purpose, to retain data for no longer than necessary and to publish a privacy policy. The rules also addressed data transfer, stipulating that the recipient must maintain the same levels of security as the sender.

The Indian government has been pushing for an EU adequacy ruling that would designate the country as data secure and opening information flows for its burgeoning IT/outsourcing industry.[14] However, this will be a difficult task until important aspects of its 2011 Rules are clarified, or a new effort is made to introduce comprehensive privacy law.

[13] *Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules*: <http://op.bna.com/pl.nsf/id/byul-8gypzn/$File/IndiaIndia.pdf> (11 April 2011).

[14] The Economic Times, *India seeks 'Data Secure Nation' status, more Hi-end business from European Union*: <http://articles.economictimes.indiatimes.com/2012-04-16/news/31349813_1_data-security-council-data-protection-laws-standard-contractual-clauses> (16 April 2012).

2.4 APEC Privacy Framework

As outlined in the first McAfee Background Paper delivered by Information Integrity Solutions P/L, development of the APEC Privacy Framework is steadily progressing. The framework aims to provide a minimum benchmark for privacy protection in and between the 21 APEC nations, modelled on the OECD Guidelines.

2.4.1 Adoption of Cross-Border Privacy Rules

After more than five years of work, the APEC Cross-Border Privacy Rules (CBPR) system was finalised in September 2011 and endorsed by APEC Leaders in November 2011 in Honolulu.

The CBPR system consists of four elements:

1. Self-assessment — An organisation self-assesses its data privacy policies and practices against the requirements of the APEC Privacy Framework. The completed questionnaire and any associated documentation are reviewed by an APEC-approved and recognised Accountability Agent.

2. Compliance review — The Accountability Agent assesses the organisation's privacy policies and practices against the CBPR program requirements. The requirements are designed to provide the minimum standard to be met to conduct the assessments in a consistent manner across participating Economies.

3. Recognition — APEC Economies will establish a publicly accessible directory of organisations that have been certified by Accountability Agents as compliant with the CBPR System.

4. Enforcement — The CBPR system is enforceable by Accountability Agents and the respective countries' Privacy Enforcement Authorities. This is enhanced by the Cross-Border Privacy Enforcement Arrangement (CPEA) which commenced in July 2010, facilitating information sharing among Privacy Enforcement Authorities and providing mechanisms to promote effective cross-border cooperation between enforcement authorities.

In February 2012, the APEC Data Privacy Subgroup identified and addressed the steps needed to implement the CBPR, paving the way for Member Economies and companies to participate in the CBPR system.

2.5 European Union

On 25 January 2012 the European Commission published its proposal for a new EU Regulation on the protection of individuals with regard to the processing and free movement of their personal data.[15] The Draft Regulation is proposed to replace the Data Protection Directive (Directive 95/46/EC) which has been in force since 1995. To address increasing technological advances, the privacy concerns of individuals and the economic interests of businesses, the Draft Regulation amounts to a major reform of the existing data protection framework.

[15] European Commission, *General Data Protection Regulation*: <http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf> (25 January 2012).

The problem with the 1995 Directive is that it left implementation of its goals to each Member State, resulting in a patchwork of different national laws — 27 rules in 27 countries. On the other hand, a regulation is directly binding on Member States and, once passed, automatically becomes part of the national law of each Member State. This will ensure that all individuals, companies and organisations will be subject to a single set of rules, regardless of where they are in the EU.

One similarity of the Draft Regulation with the 1995 Directive is coverage — it does not apply to law enforcement and national security. The processing of personal data for the purposes of investigation and prosecution of crime is covered by a new draft Directive which was released on the same date as the Regulation.[16]

The key features of the Draft Regulation include:

- Strengthened notion of consent — Consent to data processing must be 'specific, informed and explicit'. Consent can no longer be implied from silence or mere acceptance. Furthermore, there is no consent where the individual has no genuine and free choice, and is not able to refuse or withdraw consent without detriment. Data minimisation — Personal data must be limited to the minimum necessary and shall only be processed if there is no way to fulfil the purpose without using that data.

- Removal of unnecessary administrative burdens — Cutting red tape and removing unnecessary formalities such as general notification requirements for companies and organisations.

- Increased responsibility and accountability for personal data processors — Companies and organisations to conduct risk assessments, appoint data protection officers for those with 250+ employees, and adopt the principles of 'privacy by design' and 'privacy by default'. Processors will also be jointly and severally liable for the acts of the controller unless they can demonstrate no fault.

- Data breach notification — Companies and organisations to notify the data protection authority of all data breaches without undue delay, within 24 hours if feasible. Notice must be provided to individuals where there is a likely adverse affect on privacy.

- One stop shop — Companies and organisations will be answerable to a single national data protection authority.

- External application of EU law — EU rules will apply to data controllers outside the EU where the controllers' activities are related to the offering of goods or services to EU individuals, or to the monitoring of their behaviour.

- Significant penalties for violations — National data protection authorities will be empowered to deliver fines of up to €1 million or up to 2% of the company's global annual turnover.

[16] European Commission, *Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of dealing with crime*:< http://ec.europa.eu/home-affairs/doc_centre/police/docs/com_2012_10_en.pdf> (25 January 2012).

- Right of portability — Right to freely access and transfer personal data from one service provider to another. This will be particularly relevant in cases of cloud computing and outsourcing.

- Right to be forgotten — Right of individuals to have data about them deleted, when they no longer want it to be processed and there are no legitimate grounds for retaining it.

The Draft Regulation will now be discussed by the European Parliament and the Council of Ministers, with an eye to implementation in 2015. The Regulation in its current state will not only impact Australian companies with branch offices and/or subsidiaries within the EU, but more significantly, it would also purport to exercise jurisdiction over Australian companies, even if based solely in Australia, who offer goods or services to EU citizens.

The current proposal demonstrates the EU's commitment to empowering and protecting individuals and their control over personal data. However, there are many challenges ahead.

Companies have expressed unease with provisions relating to data breach notification, restrictions on behavioural targeting and the extraterritorial application of EU laws, citing concerns that the regulation could limit innovation and impose additional costs.[17] Furthermore the Article 29 Working Party, which is responsible for data protection, has written to the EU Commission's Vice-President and Justice Commissioner Viviane Reading expressing 'serious doubts as to whether the significant budgetary implications of these enhanced duties [in the Draft Regulation] are sufficiently recognised.'[18] The committee has called for an independent in-depth assessment of the financial implications of EU data protection law reform on data protection authorities.

2.5.1 THE RIGHT TO BE FORGOTTEN

The most ambitious proposal in the Draft Regulation is a legal right to be forgotten — addressed in the first McAfee Background Paper delivered by Information Integrity Solutions P/L — that is championed by Viviane Reding. It recognises that individuals should have a right to remove information about themselves, whether it is outdated, unflattering or simply because they have changed their minds. In line with what the Paper foreshadowed, the right to be forgotten is not an absolute one. The Draft Regulation has sought to balance it with public interest considerations of freedom of expression and public health, as well as with historical, statistical and scientific research purposes.

The challenge will lie in how the right to be forgotten will be implemented, in light of the dispersion of information from users to data collectors to third parties.

[17] See, eg, Financial Times, *New EU privacy rules worry business*: <http://www.ft.com/intl/cms/s/2/e14f2f3e-44f3-11e1-be2b-00144feabdc0.html#axzz1sMDlKanj> (22 January 2012); the Tech Herald, *Streamlined data protection laws in the EU raise concerns*: < http://www.thetechherald.com/articles/Streamlined-data-protection-laws-in-the-EU-raise-concerns> (23 January 2012).

[18] Article 29 Data Protection Working Party, *Letter to Vice-President Viviane Reding*: <http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2012/20120404_letter_to_vp_reding_resources_en.pdf> (4 April 2012).

2.6 UNITED STATES

2.6.1 BLUEPRINT FOR PROTECTION OF CONSUMERS ONLINE

The US also proposed a new privacy framework, with the Obama Administration announcing on 23 February 2012 a blueprint for protecting consumer data privacy and promoting innovation in the digital economy.[19] The centrepiece of the framework is a Consumer Privacy Bill of Rights ('the Bill') which applies the following principles to the commercial use of personal data:

- Individual control — Consumers have a right to exercise control over what personal data companies collect from them and how they use it.
- Transparency — Consumers have a right to easily understandable and accessible information about privacy and security practices.
- Respect for context — Consumers have a right to expect that companies will collect, use and disclose personal data in ways that are consistent.
- Security — Consumers have a right to secure and responsible handling of personal data.
- Access and accuracy — Consumers have a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity and risk associated with the data.
- Focused collection — Consumers have a right to reasonable limits on the personal data that companies collect and retain.
- Accountability — Companies should be accountable to enforcement authorities and consumers for adhering to these principles.

President Obama has called on Congress to enact legislation that would give the Bill an enforceable, statutory basis. In the meantime, the Commerce Department is convening with various stakeholders to develop codes of conduct that would implement the principles in the Bill. The codes will be enforceable once a company opts in.

The blueprint also recognises the critical role of the Federal Trade Commission (FTC) (the country's chief privacy policy and enforcement agency) in protecting consumers' privacy interests and seeks to strengthen its enforcement capabilities. Finally, the blueprint aims to improve international interoperability of protection mechanisms to facilitate the transborder flow of data.

Until concrete legislation is introduced, the challenge in the medium-term will be to draft meaningful codes that will be voluntarily abided by companies and to empower the FTC to enforce the codes.

[19] The White House, *Consumer Data Privacy in a Networked World*: <http://www.whitehouse.gov/sites/default/files/privacy-final.pdf> (February 2012).

2.6.2 FEDERAL TRADE COMMISSION REPORT ON PROTECTING CONSUMER PRIVACY

Following the release of the White House blueprint, the FTC issued a final report setting forth recommendations for businesses and policymakers to protect the privacy of American consumers.[20] In clear recognition of the privacy challenges posed by developing technologies, the report focused on five main action items:

- Do Not Track — the FTC commended browser vendors for developing tools to allow consumers to limit data collection about them, but is pushing for a stronger option to stop collection altogether that would put them at odds with the online advertising industry.
- Mobile — the FTC urged companies offering mobile services to work toward improved privacy protections including effective and accessible privacy disclosures.
- Data brokers — the Commission called on data brokers (businesses that trade data for profit) to make their operations more transparent by creating a centralised website to identify themselves and to disclose how they collect and use consumer data. The FTC has also recommended for Congress to address this.
- Large platform providers — the report highlighted the ability of platform providers such as ISPs, browsers and social media companies to comprehensively track users online and will host a public workshop in the second half of 2012 to explore the privacy issues.
- Promoting enforceable self-regulatory codes — the FTC has pledged to work with the Department of Commerce and stakeholders to develop industry-specific codes of conduct, and to enforce those codes.

The Commission resolved that the framework should not apply to companies that only collect data from fewer than 5,000 consumers a year and do not transfer that data. In light of concerns that through technological advances more data could be 'reasonably linked' to consumers, computers or devices, the report clarified that data is not 'reasonably linked' if reasonable measures are taken to de-identify the data.

Given the leading role of the US in shaping internet commerce, Australian businesses and regulators would do well to pay attention to the recommendations and future activities of the FTC.

[20] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change*: <http://www.ftc.gov/os/2012/03/120326privacyreport.pdf> (March 2012).

3 OTHER PRIVACY CHALLENGES AND DEVELOPMENTS

3.1 Do Not Track

Currently, it is standard practice for websites and myriad online companies to track individuals' web browsing behaviour by collecting information such as sites visited, likes and preferences, and online purchases. In parallel with the Obama Administration's announcement in February for a new consumer data privacy framework, the Digital Advertising Alliance (DAA) — an industry body representing more than 95 percent of online advertisers — committed to implementing a worldwide browser-based Do Not Track system before the end of 2012. This would come in the form of a machine-readable header informing websites that the user does not want to be tracked.

Consumer and privacy advocates have long called for the implementation of strong Do Not Track measures. At the same time, the online advertising industry has accepted the need for limitations on use of information but are loath to stop collecting information altogether. The industry solution proposed by DAA will prevent third-party advertisers from engaging in behavioural targeting, but will allow them to use data for market research and analytics. There will also be restrictions on the information they can collect, including users' employment, credit and health details, insurance eligibility, as well as sensitive information relating to children.

In its current formulation Do Not Track is a misnomer; a more accurate characterisation would be 'Do Not Target'. This highlights the tension facing online advertisers in balancing consumer privacy concerns with the lucrative practice of collecting and using their information. The World Wide Web Consortium (W3C), an organisation that develops international Web standards, is now actively engaged in the process of defining Do Not Track. Its Tracking Protection Working Group held a three-day conference in April 2012 and the outcomes may serve as a counterpoint to DAA's proposal, foreshadowing potential conflict in the year to come.

3.2 Big Data

The internet has revolutionised the way we connect and interact with each other, and information is its lifeblood. We are creating more data, and at a faster rate, than ever before — 90% of the data in the world today was created in the last two years alone.[21] Put simply, 'Big Data' refers to the use of voluminous, often unstructured data sets to detect patterns and extrapolate information otherwise undetectable to the human eye. The data is accumulated from a range of sources: phone and server logs, internet search terms, social media, commercial transactions, environmental sensors and financial markets, to name just a few.

[21] IBM, *Bringing smarter computing to big data*: <http://www.ibm.com/smarterplanet/global/files/us__en_us__smarter_computing__ibm_data_final.pdf> (May 2011).

Big Data has been used in a variety of innovative and surprising ways:

- Using Twitter to predict the stock market with incredible accuracy.[22]
- The uncanny tracking and shaping of customers' purchasing behaviour.[23]
- Developing an early warning signal for flu outbreaks from Google searches.[24]
- Revolutionising an entire sport through statistics analysis.[25]
- Developing the first non-intrusive test for predicting coronary heart disease.[26]

It is predicted that the market for Big Data technology and services will reach $16.9 billion in 2015, up from $3.2 billion in 2010.[27] This is an annual growth rate of 40 percent, about seven times the rate of the overall information and communications technology market. As computer processing power and outsourcing capabilities such as cloud computing continue to grow, Big Data will offer lucrative opportunities to small and medium businesses, not just large tech firms.

Big Data will be a major driving force of commercial, health and technological developments in the coming years. The implications for protecting privacy and building trust — in particular the use of data-rich profiles of individuals that can be drawn from the underlying data — will be an enduring challenge for businesses, governments and regulators.

3.3 Facial recognition

Facial recognition has had a steady if unremarkable presence in our society, mostly through its recent role in law enforcement, border control and its depiction in popular media. However, facial recognition technology is fast becoming a serious privacy concern, through the convergence of several factors:

- the growing sophistication of facial recognition software
- vastly increasing computing power and processing speed
- the ubiquity of cameras, surveillance and sensors in mobile technology; and
- the tremendous quantities of pictures and videos being uploaded every day, with Facebook and YouTube leading the charge.

[22] Wired Science, *Twitter Can Predict the Stock Market*: <http://www.wired.com/wiredscience/2010/10/twitter-crystal-ball/> (19 October 2010).
[23] New York Times, *How Companies Learn Your Secrets*: <http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html> (16 February 2012).
[24] Google, *Explore flu trends around the world*: <http://www.google.org/flutrends/>.
[25] Wikipedia, *Moneyball*: <http://en.wikipedia.org/wiki/Moneyball>.
[26] Revolution Analytics, *Complex data sets in genomic diagnostics require multiple analytic methods*: <http://www.revolutionanalytics.com/why-revolution-r/case-studies/Revolution-helps-CardioDx-accelerate-genomic-diagnostic-processes-reducing-project-time.php>.
[27] IDC, *Press Release – Worldwide Big Data Technology and Services 2012-2015 Forecast*: <http://www.idc.com/getdoc.jsp?containerId=prUS23355112> (7 March 2012).

The collection and identification of faces is attractive to governments as they seek to build databases for surveillance and law enforcement and companies see facial recognition software as another tool in the delivery of social media content and services. Facial recognition technology will also enhance the advertising sphere, where dynamic message displays can be tailored to the individual.

Broadly speaking there are three levels of facial recognition, with increasing potential for privacy intrusion:[28]

1. Simple facial detection systems that track gazes or record demographics.
2. Facial information collected on an aggregate basis and used for tailoring contextual advertisements or other messages to individuals.
3. Facial information collected individually or on an aggregate basis that is retained and linked to the individual's identity or property.

Facial recognition technology has the potential to overturn expectations of privacy, allowing anyone — be they advertisers, police or even a random stranger — to find out the identity and associated personal information of an individual with a digital image. Many companies are highly attuned to the 'creepiness factor' of such technology, as demonstrated by Google withholding its facial recognition enhancement for the Google Goggles mobile app. However, it would be naïve to think self-regulation is the answer — the problem of facial recognition will require forward thinking, including Privacy by Design concepts, from industry and regulators.

3.4 LOCATION TECHNOLOGY

Like facial recognition, location technology is gaining mainstream adoption and concern, primarily through the proliferation of mobile technology such as smartphones. Today, mobile phones track its location in multiple ways, from the inbuilt GPS device, to cell phone tower triangulation, to accessing wifi networks. When we carry our phones with us, invariably our location is almost always tracked and known.

One category of location technology involves the individual actively 'checking in' to a location. A whole industry has developed to exploit the social and commercial opportunities of sharing location data, Facebook and Foursquare being prime examples. Another category of location technology involves the delivery of services to the individual based on the passive tracking of location. Such 'location aware services' include context-specific advertising and notifications, navigation, health and fitness information, and much more.

While location technology undoubtedly provides great benefits for both consumers, government and businesses, the privacy implications are enormous. After analysing the call date, time and position records of 100,000 European mobile-users, researchers were able to forecast an individual's whereabouts with 93.6% accuracy.[29] Tech-savvy people, be they cyber-criminals, businesses or

[28] Centre for Democracy and Technology, *Seeing is ID'ing: Facial Recognition and Privacy*: <https://www.cdt.org/files/pdfs/Facial_Recognition_and_Privacy-CDT_Comments_to_FTC_Workshop.pdf> (6 December 2011).

[29] Wall Street Journal, *The Really Smart Phone*: <http://online.wsj.com/article/SB10001424052748704547604576263261679848814.html> (22 April 2011).

government authorities, can now determine our location in real-time, thereby allowing them to deduce a whole host of personal information, interests and behaviours. Meanwhile, the problem of location sharing is most vividly illustrated by the Girls Around Me mobile app.[30] The highly-controversial app — which has since been taken down — combined information gathered from Foursquare and Facebook to display for the user all females in the vicinity, including their pictures and other personal information. The fact that such information was already publicly available highlights how easy it is to overstep the bounds of what is appropriate.

Location technology is another opportunity-rich area in which eager businesses and governments are poised to make privacy mistakes.

[30] See, eg, Forbes, *Girls Around Me App Is a Reminder To Be Aware What You Share*: <http://www.forbes.com/sites/larrymagid/2012/04/09/girls-around-me-app-is-a-reminder-to-be-aware-what-you-share/> (9 April 2012).

4 CONCLUSION

Globally the pace of privacy reform has accelerated in the direction of comprehensive frameworks and regulations. Australia has been the exception, as the Government inches towards a new Privacy Act. In the meantime Australian businesses can look forward to the upcoming release of the Cyber White Paper, including the policy proposal for a national trusted identities framework. The EU and many Asian countries are set to introduce sweeping legal changes that could potentially impact Australian firms who seek and process information of their citizens. Finally, while the US has not proposed new laws, both the White House and the key enforcement agency have set out recommendations aimed at the protection of consumer privacy online. Any responses by global US firms will warrant close attention.

Technological advancements are also accelerating. Big Data enables the exploitation of data that no-one previously thought would be useful or profitable. Facial recognition and location technology are revolutionising the way products and services are personalised and delivered. However, before businesses jump on the bandwagon, they should carefully consider the many privacy implications.

2011 and 2012 have been action-packed, with technology, businesses and regulators locked in a quickening race. The global privacy landscape is more dynamic and fraught than ever before.

5 APPENDIX I: RECENT PRIVACY LAWS IN ASIAN JURISDICTIONS

Country	Law	In Force	Coverage
Taiwan	Personal Data Protection Act, 2010	No, sometime in 2012	Public and private sectors
Malaysia	Personal Data Protection Act, 2010	No, sometime in 2012	Private sector, in commercial transactions
Vietnam	Law on Protection of Consumer's Rights, 2011	Yes	Private sector, in commercial transactions
South Korea	Personal Data Protection Act, 2011	Yes	Public and private sectors
Singapore	Personal Data Protection Bill to be introduced in 2012	No	Private sector
Philippines	Data Privacy Act, 2011	No, sometime in 2012	Public and private sectors
India	Information Technology Act, 2000 and IT Rules, 2011	Yes	Private sector

Building trust and innovative privacy solutions

Information Integrity Solutions Pty Ltd
ABN 78 107 611 898
PO Box 978, Strawberry Hills NSW 2012, Australia

+61 2 8303 2438
inquiries@iispartners.com

www.iispartners.com