The Global Changing Privacy Landscape

Chong Shao, Annelies Moens and Malcolm Crompton
Information Integrity Solutions Pty Ltd
Sydney, Australia
inquiries@iispartners.com

***Abstract*—The pace of change in uses and regulation of personal information has continued to accelerate around the globe. This brief review looks at changes over the past 12 months in the regulation of handling of personal information through new or amended privacy law. Our observations are that there is an increasing recognition of privacy in the regulatory environment. Indeed, countries that have had privacy law for some time are updating their laws while countries that had not previously considered privacy law now have it in place. Australia, Korea and the EU are examples of the former described in this paper; Singapore, the Philippines and China are examples of the latter.**

***Index Terms*—privacy, privacy principles, privacy law, data protection, regulation, Australia, Asia, Europe, United States of America**

I. Introduction

Today, privacy is at the forefront of the public consciousness. It is therefore vital to keep up-to-date with the latest privacy developments. This is the third edition of the Global Changing Privacy Landscape Background Paper prepared by Information Integrity Solutions [1].

The past year has been another eventful one. The alignment of 21st century technologies with modern day needs has led to the growing realization by stakeholders in both the public and privacy sectors that data is a precious asset class. Data is the oil from which new insights, services and industries will be generated. This realization has resounded across the world and it presents exciting opportunities.

Last year's Background Paper noted that "[w]hether 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]." This statement proved to be prescient, as the recently amended Australian Privacy Act contains just such a requirement in its new privacy principles. The requirement is one of a multitude of changes taking effect in 2014 after the Parliament passed the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* in November last year, marking the first substantive update since the privacy reform process began seven years ago.

Elsewhere on the regulatory front, progress continued unabated:

- In Asia, Singapore and the Philippines have introduced comprehensive privacy law for the first time. The surprise has been China, who has taken big strides in recent months with the introduction of a law on internet data protection as well as a non-binding but nevertheless important guideline on the protection of personal information in electronic systems.
- APEC's Cross-Border Privacy Rules system is being implemented, with two countries (the US and Mexico) signing up to the framework so far.
- Europe is engaged in a complex debate over the Draft Regulation on data protection that was released in January 2012. Regulators, privacy advocates, multi-national corporations and nation states are all attempting to exert themselves on the drafting process ahead of a final vote expected before June 2014.
- While the US has been quiet at the federal legislative level, a range of privacy initiatives have been pursued by state legislators, governmental and non-governmental organizations, and the private sector. The Federal Trade Commission has also strengthened its position as an influential privacy advocate and regulator through its consumer protection mandate.

II. Recent Developments in Regulation of Privacy in Australia and Abroad

A. Australia

Undoubtedly the most noteworthy development in the past 12 months for Australia is the amendment of its 25-year-old Privacy Act. The *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (the Reform Act) was passed by Parliament on 29 November 2012 and received royal assent on 12 December 2012 [3]. The Reform Act is the culmination of a law reform process that began in 2006 with the Australian Law Reform Commission's inquiry into privacy law in Australia.

The Reform Act seeks to protect and empower individuals by placing a greater focus on openness, accountability and compliance. Significant changes have been made to the governing privacy principles, the rules underlying the disclosure of personal information overseas, the credit reporting system and the Privacy Commissioner's powers, as described below. Other ideas to come out of the reform process—including mandatory data breach notification and a statutory tort of invasion of privacy—have not yet progressed beyond the inquiry stage. The Reform Act commences on 12 March 2014, allowing for a 15 month implementation window.

978-1-4799-0540-9/13/$31.00 ©2013 IEEE

1) Privacy Commissioner's Powers

Notably for all organizations under the Privacy Act, the Privacy Commissioner has received significant new powers. The amendments enable the Commissioner to:

- Conduct assessments of privacy compliance for Commonwealth agencies as well as private businesses.
- Direct a Commonwealth agency to conduct a Privacy Impact Assessment on a project that may have a significant impact on the privacy of individuals.
- Accept and enforce written undertakings from an entity to act or refrain from acting in a certain way so as to comply with the Privacy Act.
- Recognize external dispute resolution schemes.
- Apply to the Federal Court or Federal Circuit Court to seek enforcement of a determination made as a result of an 'own motion' investigation.
- Apply to the Federal Court or Federal Circuit Court for a civil penalty order in relation to the breach of a civil penalty provision, which includes a maximum fine of $1.7 million for entities that engage in serious and repeated interferences with privacy.

The strengthening of the Privacy Commissioner's investigatory and enforcement powers is an important departure from the status quo and will lead to changes in the way privacy is recognized and regulated in Australia.

2) Australian Privacy Principles

A single set of Australian Privacy Principles (APPs) will replace the current National Privacy Principles (NPPs) for the private sector in Australian and Information Privacy Principles (IPPs) for the federal public sector. The most significant changes to the existing NPPs and IPPs are outlined below.

a) Open and Transparent Management of Personal Information (APP 1)

APP 1 not only requires entities to have a clear and accessible privacy policy, but importantly it also requires entities to take direction to implement practices, procedures and systems that will comply with the APPs. This is likely to be a sleeper issue and one that businesses would do well to take note of. Full adherence to APP 1 will not only minimize the risk and liability associated with privacy harms; it may also enhance the entity's reputation as someone who takes privacy seriously.

b) Use and Disclosure for the Purpose of Direct Marketing (APP 7)

The general rule is that an entity may use personal information for direct marketing where consent has been obtained or an opt-out mechanism is provided. Where the entity is conducting direct marketing on behalf of itself or others, an individual has the right to request the entity to provide the source of its information.

c) Cross-Border Disclosure of Personal Information (APP 8)

Several big changes are taking place. Firstly, APP 8 refers to cross-border 'disclosure' (as opposed to 'transfer' in NPP 9) of personal information. This means that APP 8 has broader application than NPP 9, since it is enough that an overseas party sees the personal information on a computer screen—the information need not be physically transferred.

Secondly, for the first time government agencies will be subject to the cross-border requirements. The existing IPPs do not contain any provisions to this effect.

Finally, the change in APP 8 signals a move away from an 'adequacy' model to an 'accountability' model of cross-border information flows. Under the current NPP 9, an entity may only transfer personal information to another country if the recipient is subject to a law, binding scheme or contract that protects the personal information in a substantially similar way to the NPPs. Subject to some exceptions in APP 8.2, an entity is required by APP 8.1 to take reasonable steps in the circumstances—typically via contractual arrangements—to ensure that the recipient does not breach the APPs. To drive home the accountability model, a new section 16C provides that where an Australian entity relies on APP 8.1 to disclose personal information to an overseas recipient not ordinarily subject to the APPs, any breaches caused by the recipient may be imputed to that entity.

d) Credit Reporting Provisions

Credit reporting has been overhauled by the Reform Act. The most profound change is the move to a more comprehensive credit reporting regime, anchored by five new categories of 'positive' information that may now be collected:

- Type of active credit account.
- Date an account is opened.
- Date an account is closed.
- Account credit limits.
- Credit repayment history.

The Reform Act introduces new responsibilities for entities handling credit information. Analogous to APP 1, credit reporting bodies, credit providers and other 'affected information recipients' (e.g., mortgage and trade insurers, related body corporates, etc.) must take reasonable steps to implement practices, procedures and systems to ensure that they comply with the Privacy Act and any relevant Credit Reporting codes. This includes having a clearly expressed and up-to-date policy about the management of credit reporting information.

The Reform Act also introduces more protections for individuals, including:

- Prohibition on the reporting of credit-related information about children.
- Prohibition on the reporting of defaults of less than $150.
- Ability for individuals to request a freeze on use or disclosure of their credit reporting information in the case of actual or suspected fraud (including identity theft).
- Enhanced correction and complaints process.

B. Asia

Important developments have taken place in the 12 months since the previous overview of privacy regulations in Asia. Now that the regulatory gaps are increasingly being filled, the

big question will be how effectively each regime will be enforced. This could vary greatly across jurisdictions and is a consideration that will be as important as the legal provisions themselves.

TABLE I.

Country	Law / Guideline	In Force	Coverage
Taiwan	Personal Data Protection Act 2010	Yes	Public & private sectors
Malaysia	Personal Data Protection Act 2010	Not yet	Private sector, in commercial transactions
Vietnam	Law on Protection of Consumer's Rights 2010	Yes	Private sector, in commercial transactions
South Korea	Personal Data Protection Act 2011 (in addition to longstanding sectoral laws)	Yes	Public & private sectors
Singapore	Personal Data Protection Act 2012	Yes, in phases	Private sector
The Philippines	Data Privacy Act of 2012	Yes	Public & private sectors
Thailand	Personal Data Protection Bill 2011	Not yet	Private sector
India	Information Technology Act 2000 and Information Technology Rules 2011	Yes	Private sector
Hong Kong	Personal Data (Privacy) Ordinance—amendments introduced in 2012	Yes, in phases	Public & private sectors
China	Decision on Strengthening Protection of Internet Data	Yes	Public & private sectors, electronic information
	Guideline for Personal Information Protection Within Public and Commercial Information Systems	Yes, but not legally binding	Private sector

Fig. 1. Privacy Law Reform in Asia

1) Singapore

Following on from the draft bill that was released in March 2012, the Singapore Government has moved quickly by passing the *Personal Data Protection Act* (the PDPA) on 15 October 2012 [4]. The PDPA establishes two 'firsts' for Singapore—a comprehensive personal data protection regime for the private sector and a Do-Not-Call registry for individuals to opt-out of direct marketing messages. Provisions relating to the registry will come into force in early 2014 and the main personal data protection rules will come into force in mid-2014.

The personal data protection regime operates upon three principles:

- Consent—organizations may collect, use or disclose personal data only with the individual's knowledge and consent, subject to certain exceptions.
- Purpose—organizations may collect, use or disclose personal data only after they have provided notice to the individual about the purposes for collection, use or disclosure.
- Reasonableness—organizations may collect, use or disclose personal data only for purposes that would be considered appropriate to a reasonable person in the given circumstances.

Organizations are obliged to appoint at least one individual to be responsible for compliance with the PDPA. For transfers of personal data outside of Singapore, the organization must ensure that the overseas recipient maintain a standard of protection comparable to Singapore law. This can be fulfilled in a number of ways, including via contract and binding corporate rules.

The Personal Data Protection Commission, established on 2 January 2013, will enforce the rules, issue guidelines and promote privacy awareness. The Commission can give directions to ensure compliance and impose fines of up to S$1 million (AU$ 775,000) for contraventions of the PDPA.

2) The Philippines

The *Data Privacy Act of 2012* (the DPA) came into effect on 8 September 2012 [5]. It is the first data protection law in the Philippines. The DPA is modeled substantially on the EU Data Protection Directive and the traditional Fair Information Practice Principles of notice, consent, access and correction. Notably, the DPA has the distinction of being one of the toughest privacy regulation frameworks in the region:

- The data subject has the right to demand a wide array of information relating to an organization's information handling process.
- The data controller must indemnify the individual for any damages sustained due to inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorised use of personal information.
- The data controller must provide for the security of the personal information, in light of the circumstances as well as 'current data privacy best practices'—i.e., this is a legislative obligation to keep up-to-date on the latest privacy developments.
- Mandatory data breach notification where a security breach causes sensitive or other information to be vulnerable to identity fraud and there is a real risk of serious harm to any affected data subject.
- No second chance and strictly liability for non-compliance with the DPA—penalties for unauthorised processing of personal information range between 1 and 3 years imprisonment and fines of up to PHP 2 million (AU$ 47,000).

As a concession to the Philippines' substantial IT and outsourcing industry, the DPA does not apply to personal information that is collected from non-Philippine residents in accordance with foreign law that is processed in the Philippines.

3) China

For a long time, China was notable for being one of the major Asian jurisdictions without overarching regulation addressing data privacy. The PRC Criminal Law and the PRC Tort Liability Law contain provisions on the unlawful use or disclosure of personal data in specified cases. However, due to

the lack of authoritative interpretations and implementing regulations, the provisions have been of theoretical rather than practical importance.

In the last few months, the picture has changed greatly. On 28 December 2012, the Standing Committee of the National People's Congress—China's top legislative body—passed the Decision on Strengthening Protection of Internet Data [6]. The law applies to network service providers and other enterprises that collect or use citizens' electronic personal information. Key requirements include:

- Obtain citizens' consent before collecting or using information.
- Clearly indicate the objective, methods and scope of collection and use.
- Preserve secrecy, integrity and security of information—prohibition on selling or illegally providing it to others.
- Controversially, network service providers are to require users to provide real identity information in exchange for providing online and telephonic services.

The other major development is a national standard on data protection that came into force on 1 February 2013, jointly released by the Standardization Administration and the General Administration of Quality Supervision, Inspection and Quarantine. The Guidelines for Personal Information Protection Within Public and Commercial Services Information Systems (the Guidelines) [7] are not legally binding, but do set a benchmark for the handling of personal information by all organizations excluding government bodies exercising a public administrative function.

For the first time, there is a formal definition of 'personal information': 'computer data that may be processed by an information system, relevant to a certain natural person, and that may be used solely or along with other information to identify such natural person.' The Guidelines also recognize sensitive personal information as information that would have an adverse impact on the subject if disclosed or altered (e.g., identity card numbers, race, religion and biometric information).

The Guidelines contain eight basic principles for handling personal information that are comparable to the Fair Information Practice Principles, comprising of: purpose specification, collection limitation, notice, consent, data quality, security, retention limitation and accountability. Notably, transfers of personal information to a third country are prohibited unless there is express user consent, government permission, or other legal or regulatory permission.

Along with the Guidelines, the Chinese government has announced the creation of the Personal Information Protection Alliance—a coalition of Internet companies, industry associations and standards centers—that will play a role in industry self-regulation as well as shaping future regulation.

The latest developments demonstrate that the Chinese government is finally taking notice of data privacy. Organizations with a link to China should pay close attention and adjust their strategy and practice accordingly.

C. APEC Privacy Framework

APEC's Data Privacy Subgroup is responsible for the development of privacy initiatives among the participating economies. Its Cross-Border Privacy Rules (CBPR) system facilitates the transfer of personal information between companies of participating APEC economies by ensuring that a company's privacy policies meet established standards for the protection of personal information [8]. Over the past 12 months, further progress has been made in the implementation of the system:

- The US became the first APEC economy to receive approval to participate in the CBPR system last July, with Mexico receiving approval in January 2013. Japan submitted its application in June 2013, with more countries to follow.
- Work is underway to develop different assessment criteria for companies that decide how the information is processed (data controllers) and those that process information on behalf of others (data processors).
- In March 2013, members of the APEC Data Privacy Subgroup met with their counterparts in the EU to discuss and develop a set of tools to facilitate data transfer for multinational companies that operate in both Europe and the Asia-Pacific.

The ongoing efforts signal a continuing international trend towards strengthening interoperability, lowering compliance costs for companies and protecting consumers.

D. European Union

The EU took a major step towards updating its existing data protection framework when it released its draft data protection regulation (the Draft Regulation) in January 2012 [9]. The Draft Regulation proposed sweeping changes to the current Data Protection Directive (Directive 95/46/EC) and is set to be a one-size-fits-all, binding law on the 28 EU member states. The complex process of deliberation and refinement is currently underway, with a final vote to adopt the Regulation likely to occur before the re-election of the European Parliament in June 2014 (with implementation to occur two years after that).

Developments to date paint a fascinating picture of the tensions that are roiling in the data debate in Europe. Arrayed on one side are those pushing for strong provisions—this includes Justice Commissioner Viviane Reding, the Article 29 Working Party responsible for data protection and EU legislative committees, as well as privacy advocates. Jan Philipp Albrecht, the rapporteur to the EU Parliament's Committee on Civil Liberties, Justice and Home Affairs presented a draft report detailing the amendments to the Draft Regulation. The report generally supports the Draft regulation while proposing more stringent requirements, including:

- Broader application of the Regulation—exemption changed from the company's composition (less than 250 employees) to the company's activities (less than 500 data subjects processed per year), a move that will encompass virtually all companies that process personal data.

- Broader concept of personal data—definition includes natural persons who can be identified or singled out, alone or in combination with associated data. This means that IP addresses, cookies and other unique identifiers will be considered personal data in most cases.
- Broader individual rights of access, data portability and objection to data practices (such as profiling).
- Tightened consent requirements—consent must be freely given, specific, informed and explicit. Companies in a dominant market position are not allowed to make unilateral and non-essential changes to its terms of service that leave the data subject with the option of merely accepting the change or abandoning the service.
- Stricter rules on profiling—defined as any automated processing intended to evaluate personal aspects, profiling can only occur with consent, when explicitly permitted by legislation or where necessary for the performance of a contract. Profiling that would have a legal effect or other significant impact on individuals is prohibited.

On the other side of the debate are those that advocate for a softening of the provisions. Among others, multinational US companies with a heavy stake in the European market such as Facebook, Google and Amazon have forcefully lobbied the EU, supported by the US government. At the same time, several EU member states—including Ireland, Germany, Belgium and the UK—have balked at some of the proposed rules, arguing that they would add unnecessary burdens to businesses and stifle the growth of the European technology sector.

Notwithstanding the volume and volatility of this debate, the real decisions on what changes will be made are likely to be taken by officials from the member states that comprise the EU's Council of Ministers.

E. United States

1) Recent Developments

In contrast to the frenetic developments across the Atlantic, data privacy was not a high priority for US federal lawmakers in the midst of an election year. On the other hand, significant developments have occurred at other levels, some involving the participation of the private sector:

- The National Telecommunications and Information Administration (NTIA) within the Department of Commerce—responsible for convening multi-stakeholder processes that address issues in the White House's 2012 Blueprint for Protecting Consumer Privacy [10]—began its first project in July 2012 with the development of a code of conduct for transparency in mobile apps.
- While legislators and industry groups remain gridlocked over the issue of Do Not Track, several Internet companies—seeing an opportunity to differentiate themselves—have taken matters into their own hands: Microsoft released Internet Explorer 10 in August 2012 with the Do Not Track option enabled by default and Mozilla's new version of its Firefox browser will block third-party cookies by default.
- The National Strategy for Trusted Identities in Cyberspace (NSTIC), a government-facilitated and private sector-driven initiative to develop smart identity solutions, established the Identity Ecosystem Steering Group (IDESG) in August 2012. It is currently working in collaboration with international partners to build an interoperable, digital trusted identities framework that would reduce transactional burdens and improve privacy.

2) The Federal Trade Commission

The Federal Trade Commission (FTC)—the chief consumer protection agency in the US—has continued to make its presence felt on the privacy regulatory scene by relying on its mandate to protect consumers from unfair or deceptive acts or practices. The FTC has been energetic in its promotion and protection of consumer privacy, focusing on three broad areas:

- Developing sector-specific guidelines and codes of conduct (in collaboration with other stakeholders).
- Using its clout to draw attention to particular privacy issues, pressure companies and influence policymakers.
- Undertaking enforcement actions for breaches of privacy based on unfair or deceptive acts or practices, and in the future, breaches of codes of conduct.

Over the last 3 years, the FTC has issued more than 50 enforcement actions on privacy and data enforcement. Notable actions in the past year include fining Google US$22.5 million—the largest civil penalty levied by the FTC—for bypassing privacy settings in Apple's Safari browser, and reaching a settlement with Path, the social-networking mobile app that was collecting information about minors and from users' address books without consent. The settlement includes a fine of US$800,000 and requires Path to establish a comprehensive privacy program and submit itself to independent privacy monitoring for the next 20 years.

In March 2013, the FTC's chairman Edith Ramirez reiterated that protecting consumer privacy will be a vital enforcement mission for the agency. Going forward she has indicated particular interest in mobile privacy, streamlining international data flows and the rise of ubiquitous data capture in everyday devices.

3) Government surveillance

Since the first draft of this paper, major developments have taken place with respect to the revelations of extensive government surveillance programs around the world.

In June 2013, it was reported that the National Security Agency (NSA)—America's foreign intelligence organization—has been conducting warrantless monitoring of Internet traffic in real-time via PRISM, an electronic surveillance program that began in 2007 [11]. The program involves the cooperation of major technology companies such as Microsoft, Yahoo!, Google, Facebook and Apple. The NSA searches PRISM data for suspicious communications between targets who are not US

citizens; however, data of US citizens are also inadvertently collected.

Subsequent reports revealed that the British Government Communications Headquarters (GCHQ) has been gathering vast quantities of online and telephone traffic by tapping the UK's fiber optic systems under a program called Project Tempora and sharing the data with the NSA, while France's Directorate-General for External Security was also revealed to be conducting PRISM-like activities.

These revelations highlight the tension for governments between respecting individuals' privacy on the one hand and, on the other, taking advantage of today's massive quantities of data to fight crime and terrorism. In every jurisdiction, privacy laws provide exceptions for law enforcement and national security activities. Furthermore, some jurisdictions such as the United States have special laws that enable surveillance [12].

While none of these issues are conducive to easy answers, two observations can be made:

- The issue of government surveillance goes beyond privacy law—since privacy must sometimes be compromised in the name of national security, the relevant question is how surveillance should be conducted: its extent, limits and safeguards, as well as oversight and accountability mechanisms.
- Government surveillance complicates the picture of a socially and commercially interconnected world—so many online applications and services people use today involve the transfer, processing and storage of data in third countries. The prospect that their personal information will be accessed by foreign governments may have an impact on the degree to which people share information, and accordingly affect the ability of companies to thrive in the data-driven age.

III. Conclusion

Until recently, many countries did not see the need to protect the privacy of the personal information about their citizens. Indeed, many saw competitive advantage in not having in place privacy law, on the assumption that less regulation would attract investment and outsourcing of data processing.

However, it would seem that the tide has turned. Countries that have had privacy law for some time are updating their laws while countries that had not previously considered privacy law now have it in place. Australia, Korea and the EU are examples of the former described in this paper; Singapore, the Philippines and China are examples of the latter.

The United States in many ways has taken a path of its own. Vigorous debates about how to protect personal information without stifling innovation and developing the law are taking place as much in the courts and actions of regulators as in formal legislatures.

These days, the story is all about who is next.

References

[1] An extended version of this paper was prepared for the International Association of Privacy Professionals Australia New Zealand (iappANZ).

[2] Information Integrity Solutions, "The global changing privacy landscape: background paper," launched during Privacy Awareness Week 2012, May 2012 and sponsored by McAfee, Inc for the International Association of Privacy Professionals Australia New Zealand (iappANZ)

[3] Australian Government, "Privacy Amendment (Enhancing Privacy Protection) Act 2012," ComLaw, 13 December 2012

[4] Personal Data Protection Commission, "The Act," 10 April 2013 <http://www.pdpc.gov.sg/personal-data-protection-act/the-act>.

[5] Republic of the Philippines, "Republic Act No. 10173," Official Gazette, 23 August 2012 <http://www.gov.ph/2012/08/15/republic-act-no-10173/>

[6] National People's Congress, "NPC Standing Committee on the decision to strengthen the network information protection," 29 December 2012 [Translated] <http://npc.people.com.cn/n/2012/1229/c14576-20051400.html>.

[7] Ministry of Industry and Information Technology, "National standards for personal information protection begin February 1," 22 January 2013 [Translated] <http://miit.ccidnet.com/art/32561/20130122/4670935_1.html>. The guidelines are not publicly available and must be purchased from the Ministry.

[8] APEC Committee on Trade and Investment, "APEC Cross-Border Privacy Rules System: policies, rules and guidelines" <http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/CBPR/CBPR-PoliciesRulesGuidelines.ashx>.

[9] European Commission, "Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)," 25 January 2012

[10] The White House, "Consumer data privacy in a networked world: a framework for protecting privacy and promoting innovation in the global digital economy," February 2012.

[11] See, e.g., G. Greenwald and E. MacAskill, "NSA Prism program taps in to user data of Apple, Google and others," The Guardian, 7 June 2013 <http://www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data>.

[12] PRISM is authorised by Section 702 of the Foreign Intelligence Surveillance Act, 50 U.S.C. § 1881a.