THE GLOBAL CHANGING PRIVACY LANDSCAPE

3RD ANNUAL EDITION

BACKGROUND PAPER

PRIVACY AWARENESS WEEK 2013

INFORMATION INTEGRITY SOLUTIONS PTY LTD

TABLE OF CONTENTS

1 EXECUTIVE SUMMARY

Today, privacy is at the forefront of the public consciousness. It is therefore vital to keep up-to-date with the latest privacy developments, and Information Integrity Solutions Pty Ltd is pleased to present the third annual edition of its Global Changing Privacy Landscape Background Paper.

The past year has been another eventful one. The alignment of 21st century technologies with modern day needs has led to the growing realisation by stakeholders in both the public and private sectors that data is a precious asset class. Data is the oil from which new insights, services and industries will be generated. This realisation has resounded across the world, including Australia,[1] 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 data 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 has been 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

- Although 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 organisations, 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.

Meanwhile, the privacy technological trends of the past year did not feature any single revolutionary advance, but rather the adaptation and/or increased use of existing technologies:

[1] See, eg, Queensland Government, *New portal revolutionises open data* (14 December 2012) Media Statements <http://statements.qld.gov.au/Statement/2012/12/14/new-portal-revolutionises-open-data>.

[2] Information Integrity Solutions, *The Global Changing Privacy Landscape* (2012), p 4 <http://www.iispartners.com/downloads/2012_PAW%20_IIS_%20iappANZ_background_paper.pdf>

- Big Data – Companies and agencies around the world are scrambling to adopt Big Data strategies. Exploration into the privacy implications of and policy responses to analytics (in particular its use in profiling) have begun in earnest

- The Internet of Things – Providing sensors and internet connectivity to even the most mundane of objects to optimise performance has moved from interesting theory to increasingly widespread reality. However, thorny questions remain over data sovereignty

- Unmanned Aerial Vehicles – The increasing use of UAVs or 'drones' for civilian and law enforcement purposes raises urgent privacy and regulation questions.

Underlying all of these developments is the level of trust that individuals feel they can place in organisations for the stewardship of their personal information. Loss of trust will have significant impacts on the growth of the digital economy and faith in government. While privacy regulations provide the foundational requirements, a key component of maintaining and *enhancing* trust is the extent to which organisations demonstrate greater respect for customer preferences, responsibility and accountability in their information handling practices. Successfully navigating the myriad privacy challenges requires intelligent business responses – this is the big question that organisations have to answer in the months and years to come.

2 RECENT PRIVACY REGULATORY DEVELOPMENTS AT HOME AND ABROAD

2.1 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. 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.[3]

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 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.

2.1.1 PRIVACY COMMISSIONER'S POWERS

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

- Conduct assessments of privacy performance 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
- Recognise external dispute resolution schemes
- Apply to the Federal Court or Federal Circuit Court (formerly Federal Magistrates Court) to seek enforcement of a determination made as a result of an 'own motion' investigation[4]
- 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.

[3] Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008) <http://www.alrc.gov.au/publications/report-108>.

[4] Previously, the Privacy Commissioner could enforce determinations made as a result of a complaint, but not its own motion investigations.

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 recognised and regulated in Australia.

2.1.2 Australian Privacy Principles

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

2.1.2.1 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 direct action 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 heed. Full adherence to APP 1 will not only minimise the risk and liability associated with privacy harms; it may also enhance the entity's reputation as one that takes privacy seriously.

2.1.2.2 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.

2.1.2.3 Cross-border disclosure of personal information (APP 8)

Several big changes are taking place, as foreshadowed by the draft principles that were released for comment last year. 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 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. Under the new APP 8.1, an entity is required 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.

However, APP 8 also recognises exceptions to the accountability model. The two most relevant ones that entities should take note of are:

- APP 8.2(a) – the overseas recipient is subject to a law or binding scheme that protects the personal information in a substantially similar way to the APPs, *and* there are mechanisms that the individual can access to enforce that protection[5]
- APP 8.2(b) – the entity expressly informs the individual that APP 8.1 will not apply to the disclosure upon their consent, and consent is obtained.

Where it is not possible or practical to rely on the above exceptions, clear requirements on the overseas entity to protect personal information and indemnity clauses are two contractual tools an Australian entity can use to contain the impact of a privacy breach by the overseas party.

2.1.3 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' (eg, 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.

In relation to disclosing credit eligibility information overseas to a related body corporate or person without an Australian link, a credit provider must take reasonable steps to ensure that the recipient does not breach the Privacy Act. Similar to section 16C, the credit provider will be held accountable for any breaches by the recipient.

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.

[5] This is a reformulation of NPP 9.

The new legal landscape for credit reporting complements the Federal Government's efforts to update national consumer credit legislation – consisting of the *National Consumer Credit Protection Act 2009*, the *National Consumer Credit Protection Regulations 2010* and the *National Credit Code* – that is currently underway.

2.2 ASIA

2.2.1 OVERVIEW

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.

The table contained in last year's Background Paper has been updated, with changes denoted in bold. Several noteworthy developments are discussed further below.

Country	Law / Guideline	In Force	Coverage
Taiwan	Personal Data Protection Act 2010	**Yes**	Public & private sectors
Malaysia	Personal Data Protection Act 2010	No	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 some long-standing sectoral data protection law)	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
India	Information Technology Act 2000 and Information Technology Rules 2011	Yes	Private sector
Hong Kong	Personal Data (Privacy) Ordinance	**Amended, 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**

2.2.2 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. 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 – organisations may collect, use or disclose personal data only with the individual's knowledge and consent, subject to exceptions such as:
    - Information that is publicly available, including business contact information
    - Information that is used for investigative purposes, business asset transactions, artistic or literary purposes, news activities, research, evaluation, credit reporting, and where it is necessary and clearly in the interest of the individual
    - Data intermediaries – organisations that process personal data on behalf of other organisations are subject to safeguard and retention obligations but not the consent obligation
- Purpose – organisations 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 – organisations may collect, use or disclose personal data only for purposes that would be considered appropriate to a reasonable person in the given circumstances.

Organisations 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 organisation 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.

2.2.3 THE PHILIPPINES

The Data Privacy Act of 2012 (the DPA) came into effect on 8 September 2012. It is the first data protection law in the Philippines. The DPA is modelled 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 organisation's information handling process, including but not limited to:

  - Sources from which personal information were obtained
  - Entity names and addresses of recipients of the personal information
  - Information on automated processes where the data will or is likely to be the sole basis for a decision significantly affecting the data subject
  - Date when his or her personal information was last accessed and modified

- 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' – ie, 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 strict 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.

2.2.4 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. 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 Standardisation 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) are not legally binding, but do set a benchmark for the handling of personal information by all organisations 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 recognise sensitive personal information as information that would have an adverse impact on the subject if disclosed or altered (eg, 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, overseas transfers of personal information 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 centres – that will play a role in industry self-regulation as well as shaping future regulation.

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

2.3 APEC Privacy Framework

APEC's Data Privacy Subgroup is responsible for the development of privacy initiatives among the participating economies. Its Cross-Border Rules (CBPR) system, outlined in the last Background Paper, 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. Over the past 12 months, further progress has been made:

- The United States became the first APEC economy to receive approval to participate in the CBPR system last July, with Mexico receiving approval in January 2013. More economies are expected to join this year.

- Work has been done to separate the assessment of companies that process information themselves (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 multi-national 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.

2.4 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. 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 27 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 begin 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 and EU legislative committees, as well as privacy advocates. On 10 January 2013, Jan Philipp Albrecht, the rapporteur to the EU Parliament's Committee on Civil Liberties, Justice and Home Affairs presented a draft report detailing 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 size (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 notification obligations – new categories include: the company's determination of legitimate interest; specific information on overseas transfers; notice when personal data is disclosed to a public authority; the existence of, logic behind and how to object to data profiling

- 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, multi-national 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 baulked 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.

2.5 United States

2.5.1 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 a presidential 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 multistakeholder processes that address consumer privacy issues in the President's 2012 Blueprint – 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

- A data access bill has been introduced in California in February 2013 that requires any business to disclose a customer's personal information upon that person's request, as well as the names and contact details of all third parties with whom the business shared that customer's information in the previous 12 months.

2.5.2 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.

This March, the FTC's new 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 HOT PRIVACY CHALLENGES

3.1 BIG DATA

Last year's Background Paper highlighted the innovative use of analytics to draw insight from large, unstructured data sets known as Big Data, a field that promises to usher in a transformative new era for commerce, health, and just about every other imaginable facet of society. Since then, the growth of Big Data insights has continued apace.

The Australian Government has taken active steps to capitalise on the data deluge. In March 2013, it released the Big Data Issues Paper[6] as part of its ICT strategy for the Australian public sector. The paper calls for addressing the skills deficit in managing Big Data, protecting the privacy of individuals and cross-collaboration between agencies to develop plans and guidelines for the use of Big Data. The Australian Tax Office has been chosen to lead the charge – it will head the new Data Analytics Centre of Excellence to examine data captured by government agencies. In relation to data captured by the private sector, the Issues Paper cautiously canvasses the intriguing possibility for agencies to use data from organisations such as Google, Twitter and Facebook in their analyses.

Globally, the major development in the past year has been the maturing conversation about Big Data and its implications, especially for privacy. Valuable insights have been generated by researchers, academics, public bodies and industry groups:

- With ever-increasing data sets, Big Data will be about (i) discovering useful correlations (instead of causations) based on probabilities (instead of certainties), and (ii) applying them to make predictions[7]
- Widespread use of Big Data will challenge fundamental concepts of privacy law, such as the definition of 'personal information', role of individual control, and the principles of data minimisation and purpose limitation[8]
- The notion that individuals can be protected through anonymisation is being heavily contested.[9]

The traditional model of privacy protection based on individual notice, consent, and predetermined purposes for use is becoming increasingly untenable. In the current environment, data is collected from multiple sources and analysed to find uses that were previously unthought-of. All this can take place without the subject's knowledge and with the data aggregated in a way that makes future identification possible.

---

[6] Commonwealth of Australia, *Big Data Strategy – Issues Paper* (2013) <http://agimo.gov.au/files/2013/03/Big-Data-Strategy-Issues-Paper1.pdf>.

[7] See especially Viktor Mayer-Schonberger & Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work and Think* (Eamon Dolan/Houghton Miffin Harcourt, 1st ed, 2013).

[8] See Omer Tene & Jules Polonetsky, 'Big Data for All: Privacy and User Control in the Age of Analytics' (20 September 2012). Northwester Journal of Technology and Intellectual Property, forthcoming. Available at SSRN: <http://ssrn.com/abstract=2149364>.

[9] See, eg, Paul Ohm, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymisation' (2010) 57 *UCLA Law Review* 1701.

One of the most vexing issues that will need to be addressed is profiling – that is, the analysis of data to make decisions about individuals. Increasingly, companies are catching on to the idea of personalised targeting and pricing. It is not inconceivable that one day they will go further and make the provision of their products or services contingent on the result of their data analysis. The prospect of an individual being denied a bank loan or insurance scheme, for example, on the basis of behind-the-scenes machinations is a real and troubling one.

In response to the rapid technological trends, the World Economy Forum has released a paper calling for a shift in focus from data collection to data usage, and to determine what "permissions, controls and trustworthy data practices need to be established that enable the value-creating applications of data but prevent the intrusive and damaging ones."[10] Recognising the dangers of drawing inferences, Tene and Polonetsky call for organisations to disclose their decisional criteria so that those impacted by adverse decisions are not left in the dark.[11]

The effects of Big Data are already being felt in the commercial, organisational and public realms. The difficult and necessary conversations to be had over the responsible, ethical and beneficial uses (and limits) of Big Data have only just begun.

3.2 The Internet of Things

The Internet of Things describes a network infrastructure in which everyday physical objects have a virtual presence. Just as computers are assigned IP addresses and connect to the Internet, *any* object is capable of doing so today thanks to microprocessors and wireless technologies. These 'things' come with sensors that collect and/or disseminate all kinds of information – eg, temperature, location, velocity, to name a few. Internet connectivity means that the data gathered can be analysed and used by a host of programs and services.

As the underpinning technology has improved and proliferated, the Internet of Things has expanded from an interesting concept to a fully-fledged, ubiquitous presence in our lives. Its scope is vast:[12]

- For the body – Baby pyjamas that provide parents with real-time information about their baby's breathing, skin temperature, body position and activity level
- For the home – Nest is a 'smart' thermostat that uses sensors, real-time weather forecasts and home activity to optimise temperature and reduce energy usage
- For industry – Sensors installed inside machinery can monitor the parts, send reports and enable owners to undertake scheduled maintenance ahead of actual failure
- For the environment – Motorised floating sensors can be quickly deployed in response to emergencies such as floods to track the movement of water, presence of contaminants and other conditions.

[10] World Economic Forum, *Unlocking the Value of Personal Data: From Collection to Usage* (2013) <http://www3.weforum.org/docs/WEF_IT_UnlockingValuePersonalData_CollectionUsage_Report_2013.pdf>.

[11] Tene & Polonetsky, above n 8.

[12] Examples taken from Postscapes, *An Internet of Things* <http://postscapes.com/internet-of-things-examples/>.

Perhaps the most recognisable object that encapsulates the Internet of Things is a pair of glasses – namely, Google Glasses. Due for release later this year, Google Glasses is a head-mounted display that allow the wearer to surf the web, take photos and videos, and overlay the surrounding physical environment with virtual information (ie, augmented reality). For example, looking at a subway station entrance will give the wearer details of the connecting lines and the times of trains that are due to arrive.

There are legitimate privacy concerns with Google Glasses – most obviously, the way it can be used to obtain inappropriate photos or videos by removing the friction of having to take out a camera and actually point it at the target. However, there are more fundamental issues not just for Google Glasses but every object encompassing the Internet of Things:

- Who owns the data – including data generated by and about individuals – that is collected?
- Who gets to access it?
- What are the risks and liabilities associated with its collection and use?
- What (if anything) can be done to address the privacy impacts of ubiquitous collection?

These questions are especially pertinent for data that is personal in nature, ranging from locations to faces to sensitive health information. Unless careful thought goes into designing both the technology and the terms of collection, access and use, the vacuuming of data will lead to large disparities of power and the potential for abuse.

3.3 UNMANNED AERIAL VEHICLES

An unmanned aerial vehicle (UAV), or 'drone', is a flying machine without a human pilot that is operated remotely. UAVs have been in use for several decades, firstly by the military and today expanding to a variety of purposes around the world such as surveillance, exploration, search and rescue, remote sensing and scientific research. They have also grown popular with a burgeoning group of amateur hobbyists, and are increasingly used for journalism and paparazzi activities.

In Australia, the commercial use of UAVs is regulated by the Civil Aviation Safety Authority (CASA) and the Privacy Act. However, recent discussions in the media have centred on the currently *unregulated* use of 'civilian drones' for surveillance purposes by private individuals and law enforcement. The prospect of highly mobile, aerial peeping Toms and security cameras proliferating in Australia is worrying enough that the Privacy Commissioner Timothy Pilgrim has called for a public debate on the use of civilian drones. So far his call seems to have gone unheeded.

In stark contrast, a robust discussion is taking place right now in the United States. Since the beginning of the year, bills that would restrict the use of UAVs have been introduced in more than 30 states. In March 2013, legal experts testified to the Senate Judiciary Committee of the US Congress on the need for new privacy laws to protect individuals from the use of UAVs.

With the use of civilian drones set to increase substantially in the coming years, it is important that the implications and restrictions (if any) on their ownership and use are carefully deliberated. The experience of overseas jurisdictions, especially the US, will be a helpful guide.

4 CONCLUSION

Recent privacy regulatory developments have built on the momentum of preceding years. Australia finally passed amendments to its Privacy Act in November 2012, introducing the most consequential changes since 2000. In particular, businesses and federal agencies should take note of the requirements in the new Australian Privacy Principles as well as the enhanced powers of the Privacy Commissioner.

In Asia, more missing pieces fell into place. Both Singapore and the Philippines adopted comprehensive data privacy laws for the first time last year, closely following the footsteps of their regional neighbours. The regulatory impulse in China has awakened with the introduction of a law on internet data protection and a guideline for the protection of personal information in electronic systems.

The battle over the EU's Draft Regulation on data regulation is well underway, with regulators and privacy advocates pushing for stricter rules while multi-national corporations and a number of EU member states push in the other direction. The picture in the US is different – the absence of activity at the federal legislative level has been counteracted by the disparate privacy initiatives that are currently being undertaken by a range of public and private organisations, each important in its own right.

Finally, the most consequential technological story in the past year has been the rise and rise of Big Data. While it is a term that is now familiar to most organisations, the implications of Big Data analytics for individuals' privacy and current privacy law are only just starting to be realised. Big Data's potential compounds with the amount of information that is available. The increased adoption of technologies that collect information – including objects comprising the Internet of Things as well as civilian drones – make Big Data analytics a powerful instrument that can be applied for both good and ill.

In this brave new world, organisations must recognise the importance of fostering trust. The innovative use of personal information is almost a prerequisite for success in today's economy. But where an organisation can really set itself apart is *how* it uses the information, within the regulatory boundaries. By subscribing to the values of fairness and respect for the individual and demonstrating accountability in its use of personal information, an organisation will best be able to reap the rewards of the new Big Data age.