THE IMPLICATIONS OF CLOUD COMPUTING FOR INFORMATION PRIVACY: AN AUSTRALIAN PERSPECTIVE

Dr Thilla Rajaretnam
School of Law,
University of Western Sydney (UWS), NSW Australia,
E-mail: t.rajaretnam@uws.edu.au

ABSTRACT

Cloud computing provides a large repository of information that is available to everyone as a service. Research in Australia indicates that 14 million people living in Australia use some form of cloud computing services, and approximately 900,000 small and medium enterprises businesses had actively used cloud computing services. As business that manage the new dimensional demands of data and cloud, there are challenges for governments in providing a robust legal framework and a pro-business environment. This is because cloud computing poses both information privacy and data security risks for users of cloud computing service. The information privacy risks relate to the use and disclosure of ‘personal information’ and ‘sensitive information’ about consumers without their consent while there is security threats from cloud computing related to data location, privileged user access, data segregation, recovery, investigative support and long-term viability and regulatory compliance. Trust and confidence in cloud computing by consumers and business using cloud computing is critical for its growth. This article explores the legal and regulatory implications for information privacy arising from cloud computing; and if new information privacy laws are needed to protect consumer information stored in the cloud and to support the growth of cloud computing industry in Australia. A comparative analysis of the privacy laws in the United States with that in Australia is undertaken to provide additional insights to understanding the legal and regulatory implications of adopting cloud computing services in Australia.

Key words: Cloud computing, personal information privacy, data security, regulation.

1. Introduction

Cloud computing services are an emerging and important part of the digital economy. According to the Australian Communications and Media Authority, approximately 900,000 (44 percent) small and medium enterprises (SMEs) had actively used cloud computing services by May 2013. Statistics also indicate that nearly 14 million people living in Australia between the ages of 18 years and over actively use cloud computing services in 2013. The most common cloud computing service used were webmail services (88 per cent), cloud based software (40 per cent); webmail services (57 per cent) and file-sharing service (43 per cent). Research in Australia further indicate that cloud computing market in Australia is likely to grow strongly and the compound growth rates for industry revenue is estimated to be between 19 to 25 percent per annum. Although there are benefits to the digital economy from cloud computing, there are threats to information privacy and data security. For example, consumers have identified that there is a lack of security (52 percent), lack of trust in companies providing cloud computing services (14 percent) and the perceived reliability of services (12 per cent). The information privacy and data security risks arising out of cloud computing been identified as some of the biggest obstacles to using cloud computing. In addition to the global concerns for privacy and data security, there are cross-border regulatory challenges for governments due to: the ubiquitous nature of the Internet, and the uncertainty about the location of the personal and sensitive data in the cloud which is complicated by the uncertainty of regulatory jurisdiction in the online environment where national laws are generally not applicable. Regulators are not able to constrain cloud services, or provide adequate information privacy protection for consumers and businesses that use cloud computing services. Cloud readiness, providing a robust legal framework and a pro-business environment are challenges for government and business that manage the new dimensional demands of data and cloud. For the future growth and development of cloud computing services, it is critical that regulators and cloud computing service providers are able to manage the new dimensional demands of data and cloud. This article explores the legal and regulatory implications for information privacy arising from cloud computing; and if new information privacy laws are needed to protect consumer information stored in the cloud and to support the growth of cloud computing industry in Australia. A comparative analysis of the privacy laws in the


3 Australian Government, Australian Signals Directorate, above n 1.

4 Australian Communications and Media Authority (ACMA). (2014), above n 2, at 1.

5 Australian Government, Australian Signals Directorate, above n 1 at 2.

United States with that in Australia is undertaken to provide additional insights to understanding the legal and regulatory implications of adopting cloud computing services in Australia. The next section provides a brief overview of cloud computing, the cloud computing models, the benefits and risks related to cloud computing.

2. Cloud Computing Service

Cloud computing refers to the delivery of hosted services over the Internet. In contrast to traditional computer applications that provide access content across the internet independently without reference to the underlying host infrastructure, cloud computing encompasses multiple computers, servers, and networks. Software developers have developed software for millions of users to consume cloud computing as a service. Cloud computing system consists of a collection of inter-connected and virtualised computers that provide one or more unified computing resource(s) based on service-level agreements established through negotiation between the service provider and consumers. A cloud computing system has the capacity to capture and process consumer information for commercial and other purposes. There are a number of types of common cloud computing service models available in the market. The three commonly used cloud computing service models are: the Infrastructure as a Service (IaaS) model; the Platform as a Service (PaaS) model; and the Software as a Service (SaaS) model. The Infrastructure as a Service (IaaS) model is a model in which the cloud computing service provider or vendor provides the customer(s) with the physical computer hardware including CPU processing, memory, data storage and network connectivity and the cloud service provider uses virtualisation software to provide this form of cloud service. The service is available to a single customer or to multiple customers (Multiple tenants) where the customer(s) is able to choose and run software applications of their choice and control and maintain the operating systems and software applications of their choice. Examples of cloud computing service providers that use the IaaS model include Amazon Elastic Computer Cloud (EC2), GoGrid and Rackspace Cloud. The second model is the Platform as a Service (PaaS) model where the cloud service provider provides the customer(s) the Infrastructure as a service and the operating system and server applications such as web servers. The PaaS model allows the service provider to control and maintain the physical computer hardware, operating systems and server applications. The customer is only able to control and maintain the software applications developed by the customer. Internet service providers such as Google App Engine, Force.com, Amazon Web Services, Beanstalk and Microsoft Windows Azure platforms provide the PaaS vendor services. The third model is the Software as a Service (SaaS) model. In the SaaS model, the customer is provided with an application that include an email account and an environment for users to access their cloud computing service via a web browser. There is no need for customers to install or maintain additions software applications. The customer is able to control and maintain limited applications configuration settings specific to users creating such an email address distribution lists. The customer is also able to access the end-user applications via a web browser and able to collaboratively develop and share files such as documents and spreadsheets. Providers of the SaaS cloud computing model include Salesforce.com, Google Docs and Google Gmail.

2.1 The Benefits and Risks

Those who use cloud computing services identified that the main benefits include: the ability to access these services across all devices (43 percent), data files remaining safe if anything happens to their computer (33 percent) and freeing up space on their personal computers (19 percent). For example, unlike traditional computer software programs, cloud computing software programmes are run by cloud servers, provide customers of the service a ubiquitous, convenient and on demand network access to a pool of configuring computing resources such as networks, servers, storage, applications and services. Cloud computing is able to provide users of the service a large repository of information that is available to everyone as a service. Businesses and consumers are able to access applications from anywhere in the globe. Cloud computing also offers businesses cost savings and improved business outcomes. As there are a range of cloud service providers, each provide is able to provide a different model of cloud computing services to a customer. Each type of cloud computing service model used depends on the customer’s needs and affordability.

The risks in adopting cloud computing vary depending on the cloud computing service models provided by the vendor or process, how the cloud vendor or cloud service provider has implemented their specific cloud services and the sensitivity of the data stored. Depending on the types of cloud service models offered to the customer, a service provider may yet customer emails, web traffic through external data storage and access personal productivity applications. The information privacy peril in

---

5. Ibid.
6. Ibid.
7. Ibid.
8. Ibid.
9. Ibid.
10. Ibid.
11. Ibid.
12. Ibid.
13. Ibid.
14. Ibid.
the use and disclosure of ‘personal information’ and ‘sensitive information’ about consumers without their consent.\(^{17}\) The customer or data subject whose personal information is being collected by a business or cloud service provider, may be exposed without their consent or knowledge.\(^{18}\) While some risks such as vetting of emails may be acceptable if consented to by some customers (for example, for those using Gmail messaging), this may not be the case if similar technologies are used to vet a businesses’ emails or sensitive data that include its data relating to trade secrets or intellectual property data. The cloud service user is also often tracked or forced to give personal information against their will or in a way in which they feel uncomfortable and this creates a lack of trust in the service provider. The data security threats from cloud computing relate to data location, privileged user access, data segregation, recovery, investigative support and long-term viability and regulatory compliance.\(^{20}\) A cloud computing service providers may not be able to ensure a secure environment and protect the data that is provided by their customer.\(^{21}\) In contrast to the traditional systems of computer usage that are on identifiable location, assigned to dedicated servers that are integrated into one’s own network, masked behind firewalls, and other gateway boundaries, cloud services are highly visible and designed to be accessible from anywhere by anyone. This attracts malicious hackers like bees to honey and make it easy for attackers to hack into the system. For businesses using cloud service, non-compliance with the cloud service provider’s enterprise policies or regulation give rise to loss of trust or legal liability. If businesses subscribing to cloud computing, fail to protect the personal and sensitive information of its customers such data security failures in the cloud may lead to lawsuits, invite investigation by regulators and undermine consumers’ trust. The next section examines the regulation of information privacy and data security. It provides an overview of the international landscape for information privacy and data security, and then contrasts this with the regulation in the United States and in Australia for information privacy related to cloud computing.

3. Regulation of Information Privacy and Cloud Computing

Concerns about the developments of information technologies include: increased collection and storage of personal information; the speed at which information could be retrieved; enhanced linkages between information systems and aggregation of personal information obtained from a variety of sources; data security and the cross border flows of personal information.\(^{22}\) There have been international efforts to protect information privacy and security of information in the form of self-regulatory industry codes, the development of fair information practices\(^{23}\) and privacy principles that may be voluntarily adopted by businesses or informed national efforts to adopt information privacy legislation. However, there are regulatory gaps that exist in the protection of personal and sensitive information about individuals. Some of these gaps and limitation in the regulation of information privacy and how policy makers have provided for cloud service across national borders are examined in the following sections.

3.1 International Landscape


17 Privacy Act 1988 (Cth) s 6 defines ‘personal information’ to mean ‘information or an opinion about an identified individual, or an individual who is reasonably identifiable: (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in a material form or not’; and ‘sensitive information’ to mean ‘(a) information or an opinion about an individual’s, racial or ethnic origin; or political opinions; or membership of a political association; or religious beliefs or affiliations; or philosophical beliefs; or membership of a professional or trade association; or membership of a trade union; or sexual orientation or practices; or criminal record; that is also personal information; or (b) health information about an individual; or (c) genetic information about an individual that is not otherwise health information; or (d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or (e) biometric templates’. The European Commission (EC), Directive 95/46/EC uses the same term as the OECD Guideline. Directive 95/46/EC defines ‘personal data’ as ‘any information relating to an identified or identifiable natural person’ while the OECD defines ‘personal data’ as ‘any information relating to an identified or identifiable individual (data subject)’.

18 Privacy Act 1988 (Cth) s 6 defines ‘consent’ to mean express consent or implied consent.


12 July 2002 concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive 2002/58/EC) provide for information privacy protection. All OECD member countries, including Australia, have endorsed the 1980 OECD Guidelines and passed national information privacy protection laws based upon the guidelines. Although non-binding on countries outside the European Union, the Directives referred to, in particular Directive 95/46/EC, have influenced privacy legislation in many countries including the United States of America and Australia.

Over the years, there have been law reform initiatives at the international and national levels to overcome some of the inconsistencies, gaps and limitations in the regulation of information privacy protection. These inconsistencies in privacy laws, gaps and limitations to privacy protection are partly due to the advanced technological developments and innovative technologies used to collect information over the Internet by individuals and businesses. For example, in early 2012, the EU unveiled its proposal to further improve data protection regulation in the EU. Subsequent to the unveiling of the EU proposal Article 29 Data Protection Working Party, Opinion 01/2012 on the data protection reform proposals, the Obama administration released its ‘Consumer Privacy Bill of Rights’ and the Federal Trade Commission (‘FTC’) issued its Final Report on the “Protecting Consumer Privacy in an Era of Rapid Change” (FTC Report 2012). In Australia, in light of rapid developments in ICTs, recent developments in international approaches to information privacy protection, particularly in Europe, the ALRC addressed the impact of ICTs on privacy and recommended that a principles-based and compliance-orientated regimes should be adopted. The recommendations of the ALRC, in 2012 the Privacy Act was reviewed by the federal government and resulted in the passing of the Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth) which came into effect on 12 March 2014.

In relation to the regulation of information privacy in cloud computing at the international level, two of the world’s largest trading partners and regulators, the United States and the European Union, are significant participants in the cloud computing industry. The European Commission’s cloud computing strategy includes a number of actions to support the implementation of the key actions on cloud computing. The European Commission has made cloud computing a priority area for research, development and innovation in the first Work Programme of the Horizon 2020 Programme; and built on its on-going international dialogues with third countries on key themes in relation to cloud computing, notably with the United States, Japan, Korea, Brazil and with a Latin American multilateral forum (ECLAC). Concrete results of these dialogues provide a foundation for Europe to benefit from a broader cloud computing market beyond the European Union.

---


33 The White House, Consumer Data Privacy in a Network World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy (hereinafter referred to as ‘Consumer Privacy Bill of Rights’).


The next section focuses on the initiatives in the United States for the regulation of personal information privacy protection generally and in respect to cloud computing. It is not within the scope of this article to examine every aspect of information privacy law in the U.S., but rather only those aspects which reflect the protection of personal data and sensitive data.

3.2 The United States (U.S.)

The U.S approach takes a different approach to regulation that in the European Union. In contrast to the EU and Australia, there is no comprehensive federal legislation in the U.S. that set minimum requirement to protect privacy and personal data.40 The U.S. has resisted calls for omnibus or comprehensive legal rules for fair information practice in the private sector.

3.2.1 Legal Rules

Legal protection for information privacy is ad hoc and on a targeted basis while industry norms has elaborated voluntary norms for fair information practices.31 As a result there is no specific regulation that limit the cross border flows of consumers’ personal data. This is because the flow of information has a large economic impact and business rely on personal information for activities and standards of fair information practices has benefits and burdens. The Federal Trade Commission (FTC) is the leading federal consumer protection agency that has regulatory authority to address failure to secure sensitive consumer data and the power to investigate and remedy unfair or deceptive business practices.52 The Federal Trade Commission Act of 2006 (‘FTCA’) prohibits ‘unfair or deceptive acts or practices in or affecting commerce.’53 In contrast to Directive 95/46/EC that provides a broad definition of personal data and special categories of personal data,54 the FTC does not define sensitive data. However it is agreed that there are five categories of data are sensitive, such as: information about children, financial, health information, Social Security numbers, and precise geo-location data.55 There is federal legislation that protect data collected by online services about children under the age of thirteen,56 data collected by financial institutions, data collected by credit reporting agencies57 and patient data by health care providers.58 Such legislation effectively define categories of personal data that is sensitive consumer data. For example, the Gramm-Leach-Bailey Act of 1999 (“GLB”)59 provides for safeguard rules that requires companies handling non-public personal information to have written information security policies that describe how a company has prepared for and plans to protect non-public personal information. In addition to the GLB, Health Insurance Portability and Accountability Act 1996 (“HIPPA”)60 also provides consumer protection in that it protects personal information and sensitive data. The HIPPA sets standards for the protection of personally identifiable health information. The regulations adopting the HIPPA, specify eighteen protected health identifiers (‘PHI) that could potentially identify a patient. There are other U.S law including discrimination statutes such as the Equal Credit Opportunity Act 61 prohibit discrimination in granting finance (loans and credit) on the basis of sex, marital status, age, race, colour, religion, national origin, or receipt of public income provide insight on what sensitive data mean.

3.2.2 Industry Norms and Business Practices

Industry in the U.S. has avoided the imposition of legal rules through the promotion of self-regulatory policies and schemes. The FTC encourages companies to implement substantive privacy protection that include reasonable data security measures and limits, sound data retention and disposal best practices. For example, the FTC recommends that companies provide consumers: with easy to use choice mechanisms that allow consumers to control whether their data is collected and how it is collected that 'Towards a thriving data-driven economy' Brussels, 2.7.2014, SWD (2014) 214 final [COM (2014) 442 final].

41 Ibid. at p. 500.
44 European Union, European Commission, Directive 95/46/EC, Art 2 defines personal data as "any information relating to an identified or identifiable natural person (‘data subject’); and identifiable person is one who can be identified, directly or indirectly, in particular to an identification number or one or more factors specific to his physical, psychological, mental, economic, cultural or social identity"; and Art 8 prohibits the processing of ‘special categories of data’ that reveal the racial origin, political opinions or religious or other beliefs, personal data on health, sex life or criminal convictions of natural persons without explicit consent.
47 Gramm-Leach-Bailey Act 1999, also known as the Financial Services Modernization Act of 1999, (Pub.L. 106–102, 113 Stat. 1338, enacted November 12, 1999) [hereinafter referred to as GLB 1999]. The GLB 1999 provides safeguard rules that requires companies handling non-public personal information to have written information security policies that describe how a company has prepared for and plans to protect non-public personal information.
49 Gramm-Leach-Bailey Act 1999 above n 47.
used; improve transparency of their data practices by providing privacy notices that are clear and concise and include statements describing the company’s data collection practices and use; and reasonable access to their stored consumer data. In addition, the HIPPA provides that the PHI must be protect from disclosure by reasonable and appropriate means including administrative, physical and technical safeguards and risk assessments. The technical safeguards required for PHI that are likely relevant to cloud service applications include those related to “passwords and keys, unique identification, digital signatures, firewalls, virus protection, virtual private networks and encryption.”

However, there is consensus that self-regulatory models have broken down and there are concerns for the privacy and security of personal information on the Internet and/or in the cloud. There are some critical limitations in the state of cloud technology and information systems management. These limitations arise for example, when the data created and/or use in the cloud is subject to hacking and attacks, long power outrages and other data centre related disasters that could have significant impact on businesses continuity of clients. For example, although technical and managerial controls may be in place to ensure a consumer’s privacy and security of personal data, it may not always be possible to implement technical mechanisms to controls in the cloud to protect the privacy and security of sensitive consumer data at all times. The cloud service provider’s the disaster recovery procedures may be inadequate and this may result in the client losing or be unable to access sensitive consumer data or other related data that is stored in the cloud service provider’s data centre as and when the customer needs the data store in the cloud. The backup service provided by the cloud service provider may also be inadequate. In addition, many cloud service providers do not provide their customers adequate information about their security policies and disaster recovery procedures related to the cloud service provider’s operations. Such practices of low transparency may be in conflict with their client’s information privacy compliance requirements. Securing personal data or sensitive data may be a problem in the cloud as identity access management systems that depend on user name and passwords built and sued to secure information on personal computers or in a network folder are not designed for interoperability. According to Morrow, information in the cloud is much more dynamic and fluid that information on a desktop or a network folder. Password fatigue often arise when consumers are required multiple passwords to secure personal and sensitive information. The cloud make it even more difficult to manage identity access as it complicates the open movement of data and accessibility of data from several different geographical locations. So a better regulation, security mechanism to adequately manage identity in the cloud and new ways to protect information will be necessary. The next section discusses privacy laws in Australia that protect personal information and sensitive information.

3.3 Australia

International recognition of privacy as an important human right does not automatically translate to privacy for Australians being recognised as an enforceable legal right in all circumstances. There is no right to privacy under the common law in Australia. Some information privacy protection exists under the Privacy Act 1988 (Cth) (‘Privacy Act’) and other federal legislation, as well as under state and territory legislation. As noted previously, the Act is significantly influenced by the OECD Guidelines and EU Directive 95/46/EC. Alongside statutory regulation, there is industry regulation in the form of Codes of Practice. Industry codes provide guidelines based upon fair information collection practices, transparency and accountability. Nevertheless concerns exist about whether the above-mentioned legislation and industry regulation are able to provide adequate

---

51 FTC Privacy Report 2012, above n 45 at 24 - 64.
56 Ibid.
57 This paper does not deal with the limited developments in the common law for the protection of privacy, which has little general impact on privacy-invasive technologies in e-commerce, nor does it consider recent debate as to whether there should be a statutory tort of privacy.
58 The Privacy Act 1988 (Cth) regulates the handling of personal information by Australian Commonwealth, ACT and Norfolk Island government agencies and certain private sector organisations. In addition to the Privacy Act, the Competition and Consumer Act 2010 (Cth) provides some protection to consumers against misleading and deceptive conduct by businesses in relation to advertising, while the Telecommunications Act 1997 (Cth), Telecommunications (Interception and Access) Act 1979 (Cth), Spam Act 2003 (Cth) and Surveillance Devices Act 2004 (Cth) provide some information privacy protection in relation to the activities of telecommunications providers, ISPs, retailers, e-marketers and direct marketers. This article does not consider state legislation which may impinge on privacy issues. Such legislation includes the Privacy and Personal Information Protection Act 1998 (NSW); Health Records and Information Privacy Act 2002 (NSW); Information Privacy Act 2009 (Qld); Personal Information Protection Act 2004 (Tas); Information Privacy Act 2000 (Vic); Freedom of Information Act 1992 (WA).
59 The Australian Privacy Principles (‘APPs’) under the Privacy Act 1988 (Cth) do not apply where there are comparable industry codes or codes under other legislation. For example, the Australian Communications and Media Authority regulate industry codes in the telecommunications sector including the Telecommunications Consumer Protection Code and the E-marketing Code of Practice. The Direct Marketing Code of Practice is regulated by the Australian Direct Marketing Association. The Do Not Call Register Act 2006 (Cth) also provides for an industry code relating to the marketing industry.
and effective protection for personal information in web servers. The literature indicates that the general view amongst privacy advocates is that there is inadequate regulation of the internet and its stakeholders.

3.3.1 Statutory Regulation under the Privacy Act

The Privacy Act sets out minimum standards or obligations in relation to the collection, use and disclosure, access to and correction of personal information which are broadly based on the eight basic principles of national application in the 1980 OECD Guidelines. It provided two sets of ‘fair information practice’ principles, one relating to the public sector (the Information Privacy Principles (IPPs)) and the other applying to private sector organisations (National Privacy Principles (NPPs)). Both the IPPs and NPPs are based on the 1980 OECD Guidelines. The Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth) now amends the Privacy Act, replacing the IPPs and NPPs with a single set of 13 Australian Privacy Principles (‘APPs’) that will apply to ‘APP entities’, that is, to both Commonwealth public sector ‘agencies’ and private sector ‘organisations’. APPs 1 and 2 require APP entities to consider the privacy of personal information; APPs 3, 4 and 5 deal with the collection of personal information including unsolicited personal information; APPs 6, 7, 8 and 9 relate to how APP entities must deal with personal information and government related identifiers, including principles about the use and disclosure (including cross-border disclosure) of personal information and identifiers; APPs 10 and 11 relate to the integrity, quality and security of personal information; and APPs 12 and 13 deal with requests for access to and correction of personal information. The single set of principles is intended to be more relevant to the future development of ICTs and enhance the protection of personal information in the online environment. A new s 2A will define one of the objects of the Privacy Act as the provision of a means for individuals to complain about an alleged interference with their privacy, while other amendments include a revised definition of ‘personal information’.

There are some key limitations on the application of the Privacy Act. This article will focus on three limitations that relate to exemptions for data collectors, the definition of personal and sensitive information and consent to the collection, use and disclosure of such information. First, the APPs impose obligations only on certain non-exempt private sector organisations involved in the collection, use and disclosure of personal information about individuals, and private sector data collectors within the definition of an ‘organisation’ in s 6C of the Act. The Act exempts individuals acting in a non-business capacity, small businesses, media organisations in the course of journalism, politicians engaged in political acts and practices, companies related to each other, specified government agencies and organisations acting under Commonwealth contract from the obligations imposed on data collectors. In relation to the information privacy of internet, e-commerce and cloud computing, the most important exemption is that of small businesses. The number of private sector small businesses in Australia during the

63 An ‘APP entity’ (defined in s 6(1) of the Privacy Act 1988 (Cth) as amended by the Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth)) must comply with the APPs set out in sch 1 of the Privacy Act as so amended: s 15. An act or practice of an APP entity is an interference with the privacy of an individual if the act or practice breaches an APP in relation to personal information about the individual, or breaches a registered APP code that binds the entity in relation to personal information about the individual: s 13(1)(a)-(b).
64 The Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth) makes no changes to the definitions of ‘agency’ and ‘organisation’ in s 6(1) of the Privacy Act 1988 (Cth).
65 Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth) sch 4 cl 1.
66 Ibid, sch 1 cl 36. Under the revised definition ‘personal information’ means ‘information or an opinion about an identified individual, or an individual who is reasonably identifiable: (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in a material form or not.’
67 ‘Organisation’ means: (a) an individual; or (b) a body corporate; or (c) a partnership; or (d) any other unincorporated association; or (e) a trust; that is not a small business operator, a registered political party, an agency, a State or Territory authority or a prescribed instrumentality of a State or Territory: ibid s 6C (definition of ‘organisation’ para (1)).
68 Ibid s 7B(1).
69 Ibid s 6C. A business is a ‘small business’ if its annual turnover for the previous financial year is $3 million or less: s 6D(1).
70 Ibid s 7B(4).
71 Ibid s 7C.
72 Ibid s 13B.
73 Ibid ss 7, 8.
74 Ibid s 7B(2).
75 There is also the exemption in favour of related companies, particularly the provision that the collection of personal information (other than sensitive information) about an individual by a body corporate from a related body corporate is not an interference with the privacy of an individual: Privacy Act 1988 (Cth) s 13B(1A).


78 Ibid. at p. 35.


80 Small businesses and not-for-profit organisations with an annual turnover of AUD 3 million or less and that are not health service providers or do not trade in personal information for benefit service or advantage are not covered by the Privacy Act 1988 (Cth) may opt-in to be treated as an organisation for the purposes of the Privacy Act and be subject to the APPs and any relevant APP code. See Office of the Australian Information Commissioner, Opt-in Register <http://www.oaic.gov.au/privacy/applying-privacy-law/privacy-registers/opt-in-register> (accessed 27 September 2014).

81 OECD Guideline, above n 24. The Guidelines define a data controller to mean: ‘a party who, according to domestic law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf’.

...one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, psychological, mental, economic, cultural or social identity.

As discussed above, the FTC does not define personal or sensitive data but provides five categories of data that are sensitive. These broader definitions extend to those who make decisions about personal data not just those who collect, store or process that data. It is the data controller that must notify the supervisory authority of the collection, processing, purpose of collection, and expected disclosure and usage of the personal data.

The third limitation relates to consent. Consent is the expression of autonomy, the right for individuals to make decisions about how they will live their lives. Consent is the mechanism by which the individual eCommerce user exercises control over the initial collection, use or disclosure of personal information. The Privacy Act 1988 (Cth) s 6 defines ‘consent’ to mean express consent or implied consent. In contrast, Directive 95/46/EC, Article 2 (b) defines ‘consent’ as, ‘any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed’. The requirement of unambiguous consent under Directive 95/46/EC provides greater protection than the Australian provisions where implied consent is frequently sufficient. Further, although the Privacy Act appears to protect individual privacy interest the legislation provides exceptions that protects the interest of businesses. The exception to the requirement for consent to the collection, use and disclosure and the cross border transfer of personal information under the Privacy Act gives rise to risk of invasion of privacy, and misuse of personal information for commercial purposes. In the online environment, when businesses are involved in data mining and providing cloud computing services it is not possible for consumers to know how their personal and sensitive information is being collected, used or disclosed and to consent to the transfer of their personal information across national borders. The collection, use and disclosure, and cross border flow of personal information is regulated under APPs 3, 4 and 5 that deal with the collection of personal information including unsolicited personal information. Under APP 3, an APP entity must not collect personal information unless such information is directly necessary for the entity’s function or activities, and APP3.3 provides that an APP entity must not collect sensitive information about an individual unless the individual consents to the collection of the information. APP6 provides for use and disclosure of personal information and provides that information collected for primary purposes must not be used or disclosed for secondary purposes without the consent of the data subject. However, APP6(7) makes an exception and provides that APP 6 does not apply if such information is used or disclosed by that entity for direct marketing purposes or government related identifiers. APP8 provides that before a non-exempt entity discloses personal information about an individual to an overseas recipient, the entity must take steps, as are reasonable in the circumstances, to ensure that the overseas recipient does not breach the APP in relation to the information. (APP8(1)). However, APP8 (2) provides that APP8 (1) does not apply to the disclosure of personal information about an individual by an APP entity to the overseas recipient if, the entity reasonably believes that the recipient of the information is subject to a law, or binding scheme that has the effect of protecting the information in a way that, overall, is at least substantially similar to the way in which the APPs protect the information and there are mechanisms that the individual can access to take action to enforce the protection of the law or binding scheme. It appears that although progress has been made to find a common ground through industry codes and development of fair information and privacy principles that may be voluntarily adopted by businesses by registering in an opt-in register as in the Australia under the Privacy Act, there are limitation on relying on technology and information system management to protect privacy and security of personal and sensitive information.

For the future growth of cloud computing in Australia, regulators must provide more adequate and effective protection for personal information and sensitive information.

4. Future Direction

Given the potential growth of cloud computing, policy makers and regulators in Australia and elsewhere aim to protect consumers’ privacy without unnecessarily restricting the growth of the cloud computing industry. There is currently international co-operation in relation to information privacy, policy towards consistent and harmonised privacy laws, enforceable legal rules and sanctions to deter the unauthorised and unlawful use of surveillance technology and the collection of personal information without the consent and knowledge of data subjects. However, regulators and policy makers must also address the most fundamental concepts of a privacy law that include: a consistent definition of personal information (or personal data); limit the exemptions for businesses from compliance with the Privacy Act, impose limitation on the secondary use and disclosure of personal information and sensitive information without the explicit consent of the data subject. The provision of a new range of infrastructure and regulatory framework with assurance of a degree of privacy offered and accountability related services will provide certification for such assurances and mechanisms for assurance on the service provider will enhance consumer trust and confidence in cloud computing. In addition, cloud computing service providers and businesses must also engage in risk management processes that balance the benefits of cloud computing with the risks that are associated with handling of personal and sensitive information about their customers that they have control over in the cloud. There is increasing awareness for the need for design for privacy from regulators and businesses. A variety of guidelines and techniques may be used by software engineers to ensure privacy and mitigate risks to privacy. Concerned consumers may and should choose to take responsibility by informing businesses of their requirements and expectations regarding privacy as to whether they expect: to be informed of any additional purposes that their personal information may be used for beyond the primary purpose of the transaction, or given the option to deny secondary or additional uses of your personal information (this option is usually provided in the form of opting-out of permitting the use of a consumer’s personal information for additional secondary uses or an opportunity to ‘opt-in’ to secondary uses); to be informed of a process that gives them the right to access any information that the business has about them,
at any point in time; or a process that permits them to challenge, and if successful, correct or amend any information held by a business about them, at any point in time; or an option to have their personal information anonymized for data mining purposes and/or, an option to conduct their transactions anonymously. 85

5. Conclusion

This article has explored the legal and regulatory implications for information privacy arising from cloud computing; undertaken a comparative analysis of the privacy laws in the United States with that in Australia to provide additional insights to understanding the legal and regulatory implications of adopting cloud computing services in Australia; and has examined if new information privacy laws are needed to protect consumer information stored in the cloud and to support the growth of cloud computing industry in Australia. Cloud computing is relatively new and it appears that there is a great deal of interest among regulators and policy makers to find solutions to questions about privacy and data security in the cloud. There has been calls for regulatory reforms in the European Union, in the United States, Australia and elsewhere for new information privacy laws are needed to protect the privacy and security of sensitive consumer information stored in the cloud and support the growth of cloud computing industry. However, cloud readiness, providing a robust legal framework and a pro-business environment are challenging for governments. This is because the Internet and cloud computing is borderless and there are regulatory gap in the online environment. As noted above, there are complexity in laws, regulatory gaps, inconsistent definition of personal information and sensitive information, and the role of consent. 86 While it appears that there is no parameter which leads a country towards better cloud readiness, there is evidence of emerging regulatory consensus on information privacy regulation in the European Union, the United States and in Australia. 87 There is currently international co-operation in relation to information privacy, moving towards consistent and harmonised privacy laws, enforceable legal rules and sanctions to deter the unauthorised and unlawful use of surveillance technology and the collection of personal information without the consent and knowledge of data subjects. However, much more still needs to be done in these areas.

Reference


86 King N. & V T Raja, V.T. (2013) above n 5, pp. 413-482.
17. *Do Not Call Register Act 2006* (Cth).
18. *Health Records and Information Privacy Act 2002* (NSW);
30. *Information Privacy Act 2009* (Qld).


47. Privacy Act 1988 (Cth)
48. Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth)
50. Personal Information Protection Act 2004 (Tas).
55. Telecommunications Act 1997 (Cth).