User Awareness and Policy Compliance of Data Privacy in Cloud Computing

Audrey Mei Yi Quah* **Uwe Röhm**

The University of Sydney
School of Information Technologies
Sydney NSW 2006, Australia
Email: {aqua9116,uwe.roehm}@sydney.edu.au

Abstract

Cloud computing is promising many technical benefits such as enhanced scalability, computing elasticity, and cost efficiency. However, with the benefits of cloud-based, hosted software platforms also comes the responsibility to data privacy. This paper investigates the data privacy issues brought about by cloud computing from an Australian perspective with specific focus on two aspects: How does cloud computing affect organisations' compliance to Australian privacy and data protection regulations? And to what extent are end-users aware of how cloud computing technologies affect their privacy?

We present the results of an online survey among cloud computing users and contrast these with the technological possibilities and the cloud provider positions. According to this survey, almost half of the end-users were unaware that they are in fact using one or more cloud services themselves already today. At the same time, the overwhelming majority of the participants (more than 90%) agreed that companies need to inform customers if they store and process personal customer information in the cloud. Cloud computing is playing an important role in the future of IT but the technology's privacy risks and the apparent user-unawareness necessitates the push for greater transparency of the technology.

1 Introduction

Cloud computing has become the central technology to outsource computing services and IT infrastructure to shared data centres. By capitalising on the increasingly cost efficient yet more powerful processors as well as the growing capacity of data storage systems, cloud computing providers were able to build massive and efficient data centres that have developed into factories for industrial scale computing services. In addition, the proliferation of fast, ubiquitous networks have allowed software to be increasingly delivered as an online service while enabling more and more devices to connect to such services (Carr 2008). Overall, not only are these new cloud computing providers able to achieve economies of scale far greater than what most companies can achieve with their own systems, but these providers also have more expertise in managing such large data centres (Armbrust et al. 2009).

In essence, cloud computing marks the disembodiment of computing power as Information Technology (IT) becomes a utility that can be consumed where and when it is required. As Nicholas Carr illustrated in his book "The switch: Rewiring the world, from Edison to Google", the World Wide Web has become the World Wide Computer (Carr 2008). Computing today no longer adopts or requires a fixed, physical form. Instead, it has relocated to the Internet's ever changing cloud of hardware and software. Each of the different computing components can be strewn across the globe, integrated through the Internet and shared by one and all. Indeed, cloud computing has been touted as a disruptive force in the IT industry which will completely revolutionise the way in which people work and companies operate.

This is an exploratory research aimed at investigating the data privacy issues brought about by cloud computing in Australia. The two core aspects to be investigated are user awareness and policy compliance from both end user-level and enterprise-level viewpoints. The concerns and attitudes of two different stakeholders involved in the cloud (namely the enterprise adopter, and the individual end user) will be explored. The main contributions of this study are summarised below:

- We conducted one of the first empirical studies of data privacy in cloud computing in Australia. This study investigates the impact of cloud computing on the IT landscape in Australia and the data privacy of its people. It discovered that the state of Australian privacy protection legislation has not kept abreast with technological changes.
- Two surveys were developed to investigate end user awareness and enterprise policy compliance with regard to data privacy for cloud-based IT services. The findings of these two surveys revealed the privacy concerns and practices of both end users and enterprise adopters in their use of cloud computing services. It also revealed the ineffectiveness of common privacy protection mechanisms on the Internet such as privacy notices and privacy seals.
- As part of this study, we developed a list of recommendations for the enhancement of information privacy protection with regard to cloud computing in Australia. Recommendations include the need for greater transparency in the handling of personal information in the cloud as well as the need for more stringent transborder data flow legislation in Australia.

The rest of the paper is organised as follows: The next section gives an overview of the different flavours of cloud computing and of the core technical and legal background. Section 3 describes the two surveys that we conducted and how we analysed the results.

*This work was done while the author was affiliated with the University of Sydney.

Section 4 discusses the main results of the end-user survey, while Section 5 discusses those of the enterprise survey. Section 6 concludes.

2 Background

The term "cloud computing" was introduced by Google Inc. Chief Executive, Eric Schmidt, in 2006 and since then, the interest in this approach has increased dramatically. Cloud computing is currently one of the top technology trends and Gartner has even seen fit to label cloud computing as a "transformational" technology that stands to completely revolutionise the IT industry (Gartner 2010). The cloud computing industry is primed for strong development all the way till 2014, when Gartner forecasts worldwide revenue to reach US$148.8 billion. From a local perspective, analyst firm International Data Corporation (IDC) reported in 2010 that 20% of Australian companies are looking to adopt cloud services within the coming year, while a further 45% will implement the technology after 12 months (Hutchinson 2010).

As cloud computing has gained momentum in recent years, many big players such as Google, Microsoft, and Amazon now offer their own forms of cloud services. One popular definition is by the National Institute of Standards and Technology (NIST). Their 15th revision states: "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction" (Mell & Grance 2009).

All in all, the commonality found in the various definitions is that cloud computing offers shared infrastructure where scalable and elastic, service-based offerings can be delivered to customers, on-demand and on a metered-basis. Users will no longer need to purchase and maintain their own resources, be it software or hardware, and instead will be able to lease computing resources from cloud providers.

2.1 Deployment Models

We can distinguish three different deployment models of cloud computing.

Public Cloud. This is the standard model that is most commonly associated with cloud computing. With public clouds, the cloud infrastructure and applications are owned by the service provider whom is offering cloud services on a subscription basis. These services are made available to the general public or a large industry group via the Internet (Hall 2009, Mell & Grance 2009, O'Neill 2010). Although public clouds are equipped to deliver the best economies of scale, their public nature poses privacy and security risks that can limit enterprise adoption.

Private Cloud. In this model, the cloud infrastructure is operated for the exclusive use of an organisation. The private cloud can be managed by the organisation themselves or by a third party. The infrastructure does not necessarily have to be located on-site and can exist off-site as well, such as Amazon's Virtual Private Cloud (Mell & Grance 2009, Amazon 2012*b*). It is commonly believed that private clouds can deliver some of the accessibility and scalability benefits of cloud computing without the pitfalls (O'Neill 2010, Foley 2008). Given that the organisation owns the entire private cloud environment, it has full control of all the IT resources and is responsible for the safety of their data behind company-built protections (Hall 2009).

Hybrid Cloud. Hybrid clouds utilise a combination of two or more private or public clouds. A hybrid strategy offers a solution to some of the trust issues of a public cloud, while enabling organisations to take advantage of the benefits. An organisation can decide on what sensitive data to keep secured on their private cloud while connecting to a public cloud to make use of the unlimited scalability offered for non-sensitive tasks (Hall 2009, O'Neill 2010).

Private and hybrid clouds are not examined further in this research, which concentrates solely on the investigation of public clouds. This is because public clouds present an environment where the user's data and applications reside on cloud infrastructure which is owned and maintained by a third party. It is this characteristic of the public cloud that raises the most concerns in regards to data privacy, hence the focus of this research.

2.2 Service Models

As an orthogonal aspect to these deployment models, cloud computing services can be delivered at different layers of abstraction:

Software-as-a-Service (SaaS) This approach features complete, turn-key applications running on cloud infrastructure that provide alternatives to locally run applications. Apart from limited user-specific application configuration settings, the consumer does not manage or control the underlying cloud infrastructure. SaaS applications are accessed through a thin client interface such as web browsers. Examples include the online alternatives of office applications such as GoogleDocs and the Customer Relationship Management (CRM) solution provided by Salesforce.com (Salesforce 2012).

Platform-as-a-Service (PaaS) The services at this layer provide consumers with application development environments which they can access and utilise via the Internet. Consumers can use programming languages and tools supported by the provider to deploy their created or acquired applications onto the cloud software platform. Among some well-known examples of PaaS are Google App Engine, Force.com and Microsoft Windows Azure (Google 2009, Microsoft 2012).

Infrastructure-as-a-Service (IaaS) With IaaS, cloud providers are able to deliver a complete computer infrastructure via the Internet. At this layer, consumers are able to obtain processing capacity, storage, networks and other fundamental computing resources which they will use to build their systems. Amazon EC2 is a well-known example of an IaaS offerings (Amazon 2012*a*).

2.3 Data Centre Locations

Ultimately, data that is sent to the cloud exists on physical servers in data centres operated by the cloud provider. Figure 1 shows the publicly known locations of data centres run by Amazon, Microsoft and Google (Amazon 2012*a*, Google 2009, Microsoft 2012). These companies are vague and non-specific about the exact location of their data centres and the markers shown only represent the compilation of best information available as of 2010. Furthermore, the data centre locations shown may not necessarily be utilised to provide cloud computing services.

As illustrated, there is currently a lack of cloud infrastructure in Australia and this has been one of

Figure 1: Possible data centre locations of cloud computing providers.

the main issues hampering cloud computing adoption in this country. Although Amazon and Microsoft have launched data centres in Singapore to cater for their users in the Asia Pacific region, it is uncertain whether Singapore is the most suitable location for Australian cloud adopters from a privacy protection standpoint. At present, data protection in Singapore is regulated via industry-specific laws but there are no overarching data protection or privacy laws similar to those that exist in Australia (Svantesson & Clarke 2010).

2.4 Privacy Protection Legislation

In 1980, the Organisation for Economic Co-operation and Development (OECD) published their *Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data*, an international guideline that has since proven to be instrumental for the enactment of privacy laws around the world. These guidelines have been incorporated in national legislation both within and outside the OECD, but there are still differences in the regulatory framework where the laws or lack thereof in different countries can pose serious problems for the transnational and multinational firms that conduct business worldwide (Rudraswamy & Vance 2001).

Privacy in Australia is governed by the Privacy Act 1988 (Cth) (the Privacy Act), whose provisions are influenced by the guidelines set out by the OECD (Australian Government 2010b). The type of privacy covered by the Privacy Act is the protection of people's personal information. In essence, personal information is any information where an individual is reasonably identifiable, i.e. information that identifies or could identify the individual. Aside from well-known examples such as one's name and address, personal information also includes medical records, bank account details, photos, videos, and even information about one's preferences and opinions.

2.5 Cloud Computing and Data Privacy

In Australia, businesses covered by the Privacy Act may choose to be bound by a privacy code approved by the Federal Privacy Commissioner. These National Privacy Principles (NPPs) aim to ensure that organisations that hold information about people handle that information responsibly (Australian Government 2010b). The NPPs were designed in a way that is technology neutral. As such, these laws do not specifically address cloud computing-related privacy issues, and accordingly, it is a matter of applying existing privacy laws to this new technology. Australian enterprises are responsible for how they collect, use and disclose personal data relating to their employees, customers and other business contracts. For example, NPP 4 requires that an organisation take reasonable steps to protect the personal information it holds from misuse and loss, unauthorised access, modification or disclosure (Australian Government 2001). With traditional on-site computing, an organisation asserts control over its own data. Even with business functions that are outsourced, the organisation usually still has knowledge of how their data is used and where it is physically located. The situation becomes more opaque when organisations outsource to the cloud.

When a company decides to adopt cloud services, they give their provider access to four types of data (Mowbray 2009), namely:

Customer data — Data about the organisation's own customers e.g. customer details and purchase history.

Account data — Company information e.g. the business' contact details and payment information.

Operation data — Data generated by the operation of the cloud computing services, e.g. the overall set up of the company's IT system on the cloud and the internal state of the hosted applications.

Activity data — Data from tracking when and for which applications the business' account with the service provider is used.

As such, users have a lot at stake when utilising cloud computing, and expect their personal information to be handled with due care and discretion.

As mentioned previously, one of the most contentious issues with cloud computing is the location of the cloud itself, where users often do not know where their information is being stored (Clarke 2010). Most data centres at the moment are located in US and EU, and providers may not offer specific geographic coverage to their users. This means that sensitive data about a company and its customers may be stored in an offshore location where it is now subject to different privacy laws (Mowbray 2009).

NPP 9 is particularly significant in this context because it limits the circumstances in which an organisation may transfer information about an individual to an entity in a foreign country. Transborder data transfers can only be made in circumstances such as with the consent of the individual, or for the fulfilment of a contract with the individual or in the individual's interest (Australian Government 2001).

3 Approach

This study aims to explore the opinions and behaviours of both end-user and enterprise-users with regard to data privacy in cloud computing. To this end, we conducted two web surveys over the Internet to obtain fast and inexpensive responses. However, we note that this method does have well-known disadvantages including low response rates and incomplete answers (Neuman 2006). The opt-in nature of the survey can also introduce bias into the results because the people who choose to respond may actually differ from those who do not respond. Nevertheless, as an exploratory research project, the questionnaire survey method allows us to obtain useful insights into the cloud computing environment in Australia.

3.1 Survey Tool

The two surveys were designed using Survey Monkey, a web-based survey tool which offers various pre-configured question types and advanced answer validation (SurveyMonkey 2012). All the survey responses were collected anonymously.

The end-user survey consisted of 45 questions which were grouped into nine separate sections that each covered a specific area of interest. This ranged from questions on the background of the participant's Internet usage and some demographic details to the users' data privacy expectations and their experience with privacy policies and the privacy protection in Australia.

The enterprise survey consisted of 59 question in ten separate sections. It evaluated the applicability of the Privacy Act 1988 (Cth) and asked participants about current and future cloud computing plans of their organisation. The survey's core sections dealt with the organisation's attitude towards data privacy in the cloud and the current privacy practices in the organisation regarding collection and use of customer information.

3.2 Sample Selection

Both surveys used a combination of *purposive sampling* and *snowball sampling* to recruit respondents. Both are forms of non-random sampling, where the sample size was not determined in advance (Neuman 2006).

The end user survey targeted end users who might have had experience with cloud computing technologies. To this end, emails invitations were sent out to different groups of participants, including University students and business end users from various Chambers of Commerce across Australia. In addition, a publicly available link to the survey was made available on the School of IT website. Social sites such as Facebook and Whirlpool were also used to publicise the survey.

The enterprise survey on the other hand, targeted enterprise IT decision makers that would be able to provide informative insights into the adoption of cloud computing in Australia. Email invitations were sent out to a compiled list of industry contacts. For the original contacts that did not fit the criteria of being IT managers in their companies, their assistance was requested to forward the email to other colleagues who would be better suited to complete the survey.

3.3 A model for end users attentiveness to privacy notices variable and measures

In the literature, authors stress the importance of end users reading the terms of service and privacy notices displayed by Internet-based services before actually using them (Burghardt et al. 2009, Earp et al. 2005, Gellman 2009, Vail et al. 2008). As such, the end user survey also contained suitable measurements to study their effects on an individual's attentiveness to privacy notices. Participants were asked to rate using a 5-point Likert scale: (I) Their attentiveness towards privacy notices, (II) their attitude towards privacy notices, (III) the readability of privacy notices, (IV) their trust towards website and (V) their trust towards privacy protection in Australia. The instruments to measure the variables I to IV were adapted from the work of Milne & Culnan (2004) while the items for variable V were adapted from those used by The Gallup Organisation (2008).

3.4 Data Analysis

On the survey results, the following analyses were carried out using Statistical Package for the Social Sciences (SPSS) version 19.0 software:

- Descriptive statistics (min, max, means and standard deviations) were computed to examine the normality of each of the variables.
- Cronbach's alpha coefficient to test the internal consistencies of the independent and dependent variables.
- Pearson's correlation and multiple regression analysis to analyse the relationship between the dependent variable (Attentiveness towards privacy notices) and the independent variables (Attitude towards privacy notices; Readability of privacy notices; Trust towards website; Trust towards privacy protection in Australia).
- Non-parametric tests of differences in end user concerns by age and IT expertise.

4 End-User Survey

In the following, we are discussing the results of the end-user study that explored the attitude and knowledge of Australian end-users towards cloud computing services.

4.1 Survey Size

A total of 217 responses were collected online using a online survey tool (surveymonkey.com) between 1 October and 15 October, 2010. However, only 162 responses were fully completed and of these, 9 did not qualify as they came from participants outside of Australia. Hence, the total sample size of this survey was 153 participants.

Most of the respondents were young, well-educated and experienced Internet users in Australia. The majority of them are from the 18-29 age group (67.3%), 69.3% of them possess a Bachelor's degree and above, work in the Information and Communication Technology industry (26.1%) and are Australian citizen's (57.5%) from NSW (75.2%). In addition, most have been using the Internet for 10 years or more (71.9%), classify themselves as having intermediate IT knowledge (54.2%) and utilise the Internet mainly for email (98.0%) and education (85.0%) purposes.

4.2 Descriptive statistics

Although the sample size seems to point to an IT experienced group, prior to the survey, 38% of participants had never heard of cloud computing and 46% did not know what the term meant (Figure 3). After being given a brief description of what the cloud encompassed, 86% stated that they are already using cloud computing services. It can also be observed that many end users do not fully understand the technology and thus were unable to decide if cloud computing made the protection of personal information more difficult (35%). Furthermore, the majority of end users (64%) did not know where their data was stored after being sent into the cloud.

The survey also asked respondents about their use of various Internet-based services. Figure 2 shows that respondents were more familiar with popular SaaS type applications such as email, social networking sites and online media storage, but less so with professional social networking sites and online office suites. Newer cloud services were also fairly unknown to the respondents with many stating that they had

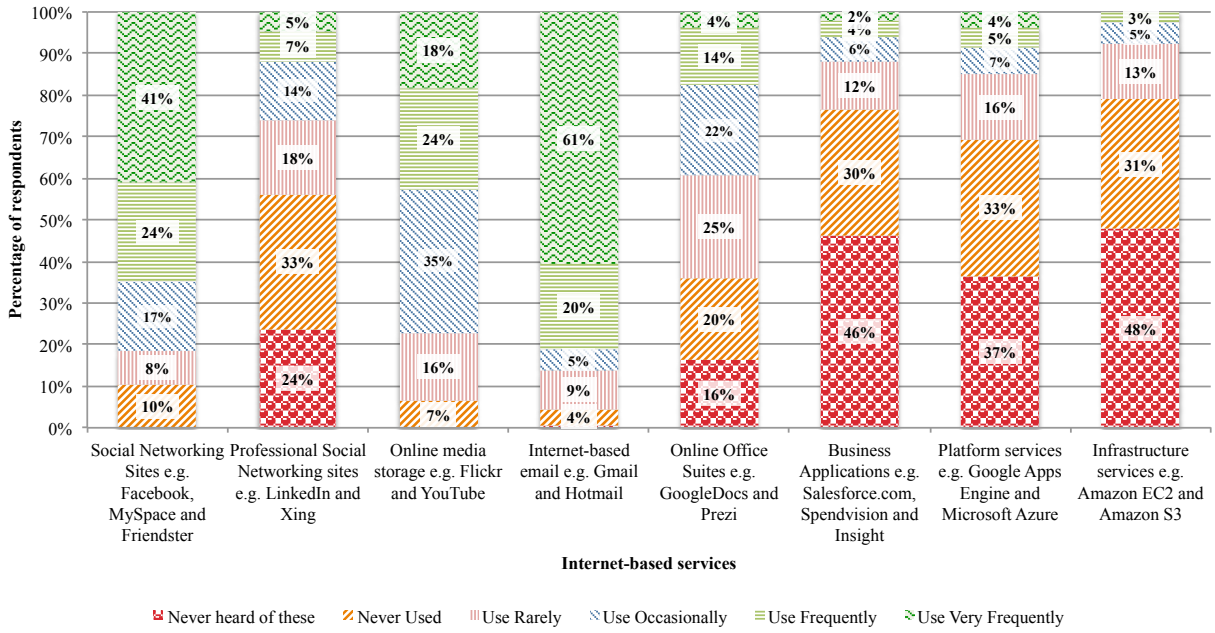

Figure 2: Use of Internet-based services.

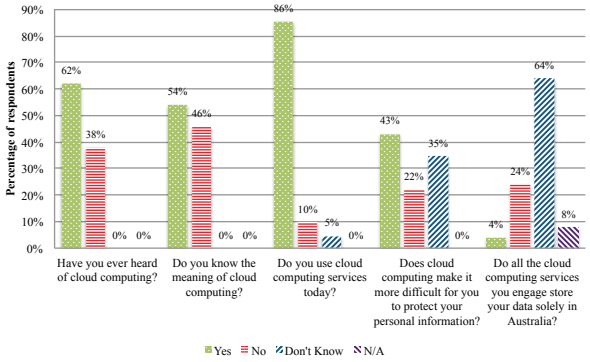

Figure 3: Knowledge and use of cloud services.

never heard of business applications (46%), platform services (37%) and infrastructure services (48%) respectively.

4.3 End-User's Privacy Expectations

We asked the respondents to rate the level of privacy they place on different types of information about themselves, on a scale from 1=Public to 5=Very Private. Figure 4 shows the mean values of the responses obtained. Respondents on average rated tax file number and credit card details as the two most private types of information about themselves.

With two further questions, we asked the participants about their opinion about privacy on the Internet in general and for their personal privacy in particular. On the whole, the respondents were concerned with the state of their personal information on the Internet, and agreed that consumers had lost control over how companies use and collect personal information. 74% of respondents also stated that they were concerned about companies storing and processing their personal information in a cloud environment without their knowledge and 90% agreed that companies need to inform customers if they send customer information into the cloud. Interestingly however, end users do not particularly value having the knowledge or control over the location of their information when using Internet- based services (Figure 5). This unanticipated finding is further substantiated via the results of the enterprise survey which revealed that organisations place relatively low importance on customers knowing and having control over where their information is stored (Figure 6, discussed in Section 5.5).

This suggests that in spite of their professed concerns, end users are not too concerned about how data location actually affects their privacy. Privacy law is specific to each country and even if an individual was able to gather sufficient information about a privacy violation, it is often difficult, slow and expensive for victims to pursue action where the violation has occurred outside the victim's home country (Clarke 2010, Svantesson & Clarke 2010). However, another possible explanation is that end users are actually aware of transborder data flow issues but have merely become too complacent and reliant on such global Internet services that they no longer care where their data is stored. This presents the classic case of benefits and convenience outweighing the risks.

4.4 The Value of Privacy Notices and Privacy Seals

This previous observation is further substantiated in Figure 7 which illustrates the end user responses regarding how often they read privacy notices for various purposes. 60% of end users state that they usually or always pay particular attention towards privacy notices when they are using their credit cards for online shopping. However, for all the other reasons presented, the majority of respondents reported that they seldom read privacy notices. These results were analysed with Cronbach's Alpha to test for equivalence reliability i.e. to analyse the degree of consistency among the items in a construct (Neuman 2006). The general rule of thumb is that a Cronbach's alpha score of above 0.7 indicates acceptable consistency. All the constructs tested in this study were above this value, thus showing acceptable reliability.

The study also studied the effect of end user's trust towards websites on their attentiveness to privacy notices and Figure 8 illustrates these findings. End users' prior experience with a company is a determining factor that disinclines users from reading the website's privacy notice. Reputation can also be seen to inspire end user trust as 55% of respondents state

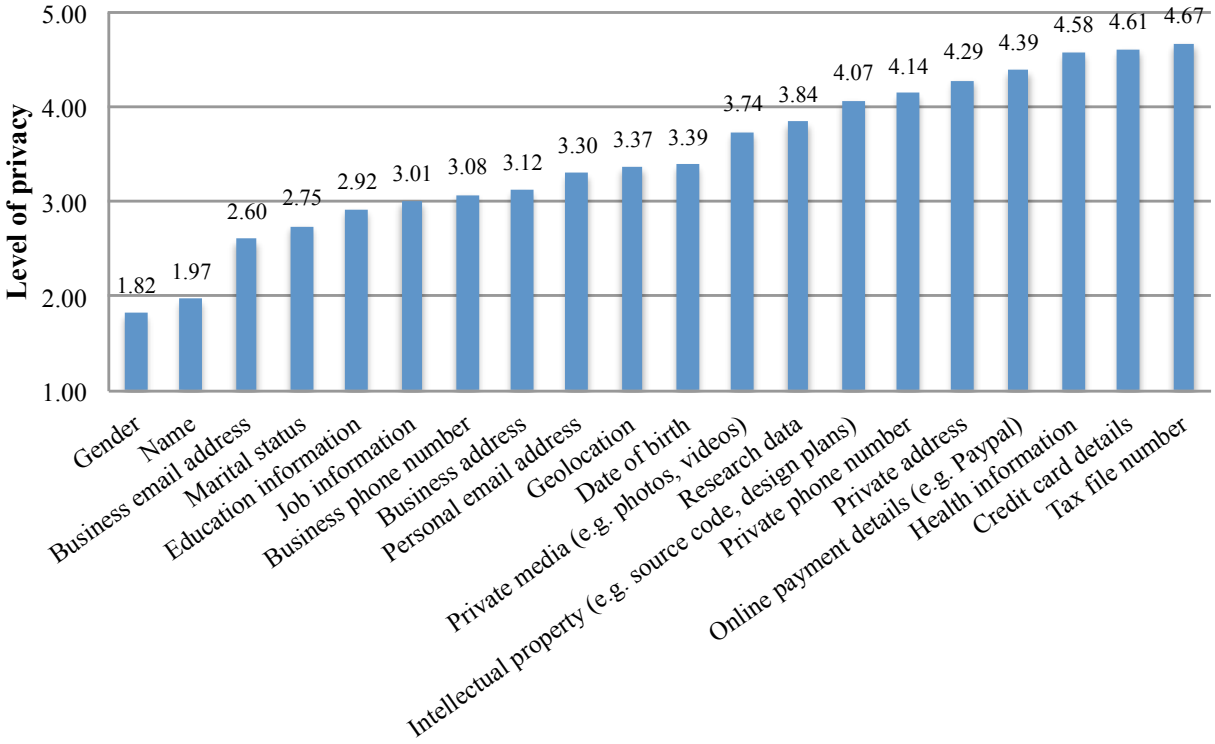

Figure 4: How end-users value privacy of information.

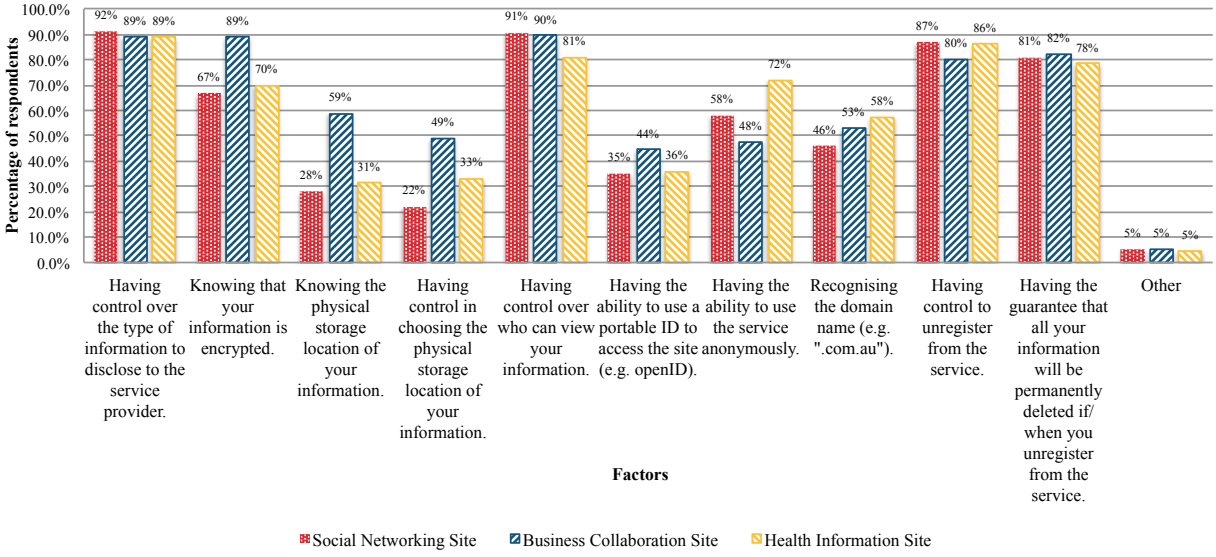

Figure 5: Important factors for end-users when using different Internet-based services.

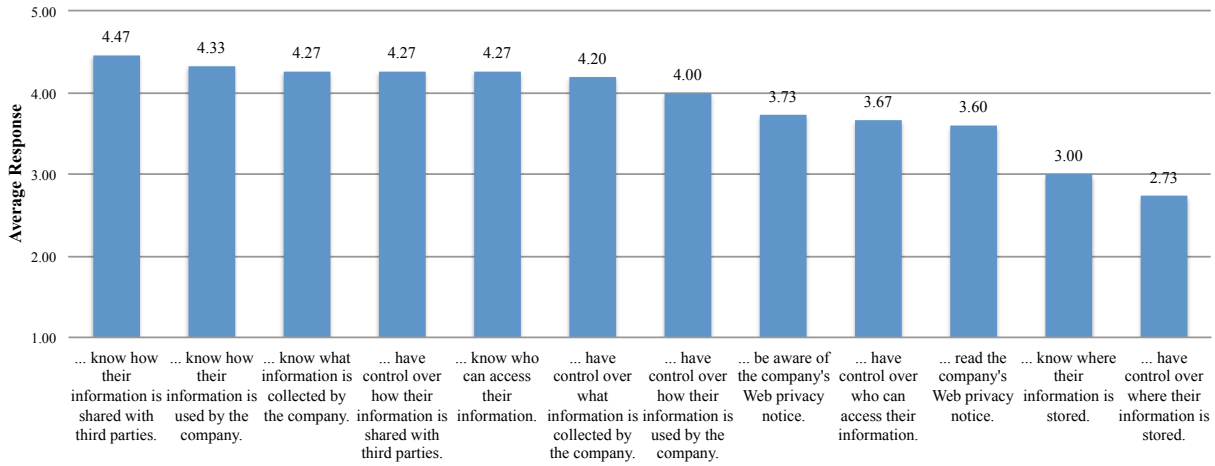

Figure 6: Practices deemed important to organisations in regards to customer information.

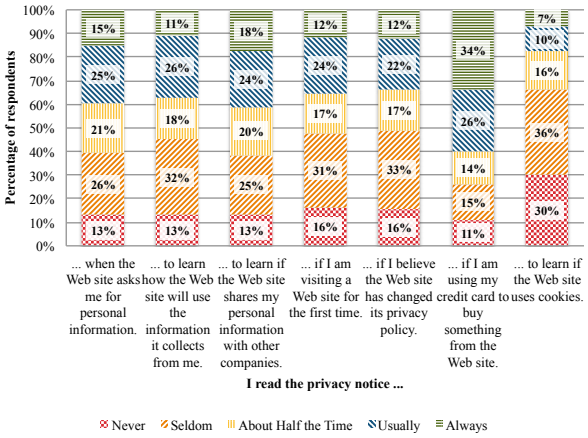

Figure 7: Attentiveness towards privacy notices.

that they do not read the privacy notice if the website belongs to a well-known company. However, privacy seals do not appear to play a major role in the privacy notice reading habits of most end users (40%) — this means that the display of a privacy seal on websites neither encourages nor discourages the majority of respondents in reading privacy notices.

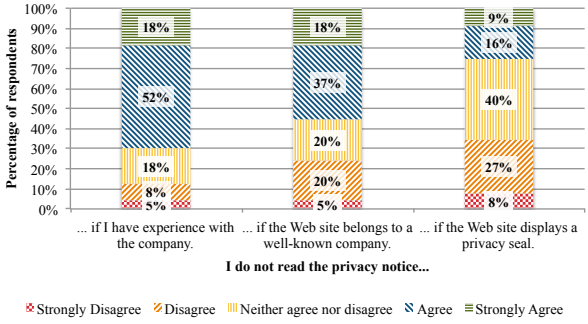

Figure 8: Attentiveness towards privacy notices.

4.5 Analysis

The survey findings demonstrate that most of the end users surveyed were new to the concept of cloud computing even though the majority were frequent users of social networking sites and online media storage, both of which are examples of the SaaS model. The popularity of such SaaS applications is consistent with the sample demographics which consisted of mostly 18–29 year old respondents. However, the overwhelming response to the survey question regarding the storage of data within Australia was "Don't Know" (64%). Respondents who responded in the negative on the other hand, mostly nominated the United States as a likely location of where their data is stored. Although it is a logical conjecture that American-owned companies such as Google and Facebook conduct their operations out of the US, this is not necessarily the case considering the global network of data centres operated by such large IT companies (cf. Figure 1).

This suggests that end users may not be fully aware of the privacy risks that exist in the cloud, most of which centre around the issue of transborder data flow. 22% of end users believed that cloud computing did not make it more difficult to protect personal information while 35% could not decide on the matter. Data that is stored in US data centres are subject to the USA Patriot Act through which the US law enforcement can obtain electronic records of users (Gellman 2009). The end users do not seem to consider such government investigations to be a major issue, but were more concerned with provider misuse of data and hacking attacks.

The survey contained several more detailed questions. For space reason, we summarise the most important findings in list form:

- The risk of data being accessed in government investigations does not appear to be a major issue concerning end users.
- The majority of respondents place low value on having knowledge and control over the location of their information when using Internet-based services.
- A good proportion of end users reported that they were uncertain of the existence of an independent authority in Australia governing data protection laws.
- The majority of respondents mistakenly believe that they have access to courts for data breaches and have the right to compensation for such privacy violations.
- Respondents below the age of 30 show more concern for the risk of data theft via external attacks compared to those 30 years old and above.
- Intermediate level IT users show the most concern for the risk of data theft via external attacks, followed by beginner level users and finally expert users.
- Attitude towards privacy notices and readability of privacy notices positively impacts an individual's attentiveness to privacy notices. On the other hand, trust towards websites negatively impacts this attentiveness. Trust towards privacy protection in Australia has no effect on attentiveness to privacy notices.

5 Enterprise Survey

A second aspect of our study is to compare the end-users perspectives with those of cloud service providers. To this end, we conducted a separate survey of enterprise users. We asked about business users' attitude towards cloud computing platforms and data privacy issues arising from the use of web-based technologies.

5.1 Survey Size

A total of 22 responses were collected. However, only 17 responses were fully completed and of these, 2 did not qualify as their organisations were not covered by the Privacy Act 1988 (Cth). Hence, the total sample size of this survey was 15 participants.

The majority of respondents have held a technical role in ICT within the last 10 years (80%), and 26.7% of them possess a Master's degree in ICT. Approximately half of the respondents (46.7%) have held a Senior Executive IT position in their respective companies, and are currently working in an Australian-owned organisation (86.7%) in either the Financial Services industry (33.3%) or ICT industry (33.3%).

5.2 Descriptive Statistics

66.7% of the IT decision makers surveyed reported that their organisations currently used cloud computing, with cloud services fulfilling less than 25% of current IT requirements in most cases (90%). For

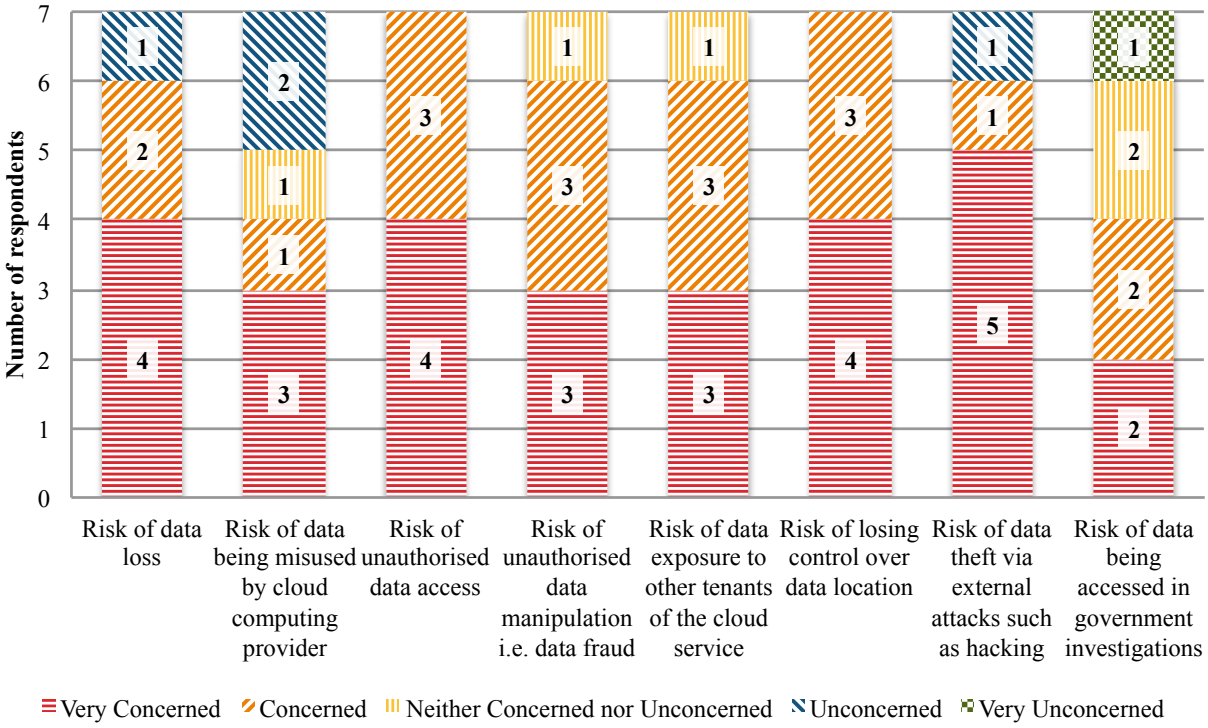

Figure 9: Enterprise concerns with storing or processing customer-related information in the cloud

businesses that have not yet utilised cloud computing, most have no strategic plans to adopt cloud computing in the future (80%). However, for enterprises with future cloud plans, they estimate that cloud computing will fulfil a higher proportion of their IT requirements in the next 3 years.

5.3 Perceived Disadvantages of Cloud Computing

Enterprise respondents were asked about the factors they considered to be disadvantages to cloud computing. These findings are shown in Figure 11 with scale of 0=Not a disadvantage to 5=Very major disadvantage. Respondents whose companies had future plans for cloud computing (N=11) on average named "data privacy risk" to be the biggest disadvantage. This is then followed by "risk of regulatory non-compliance" and "security risk" in the cloud. At the other end of the spectrum, cost was clearly not a disadvantage for respondents with regard to cloud computing.

The issue of data privacy risks with storing or processing customer-related information in the cloud was further explored with respondents in the enterprise survey. Among respondents who believed that cloud computing made it more difficult for organisations to protect customer-related information, their biggest concerns were the risks of unauthorised data access and losing of control over data location (Figure 9). Enterprise respondents were surprisingly not too concerned about data misuse by cloud providers and of data being accessed in government investigations.

5.4 Factors Influencing Cloud Adoption

Enterprise respondents were asked about important criteria that would influence their organisation's decision whether to adopt cloud computing services. It is interesting to note that having local data centres seem to be of lower importance to the enterprise respondents surveyed where 3 out of 15 respondents (20%) reported that it was not an important consideration at all (Figure 10). The most important factor in enterprise decisions to adopt cloud services is the availability of legal or indemnification agreements, with all respondents stating that it is either Important or Very Important. This is consistent with the findings of another survey question regarding the procedures that enterprises have in place to ensure the safe-sharing of customer-related information with cloud computing providers. The respondents named indemnification agreements the most often used protection when the enterprise respondents send customer information into the cloud by a slight margin.

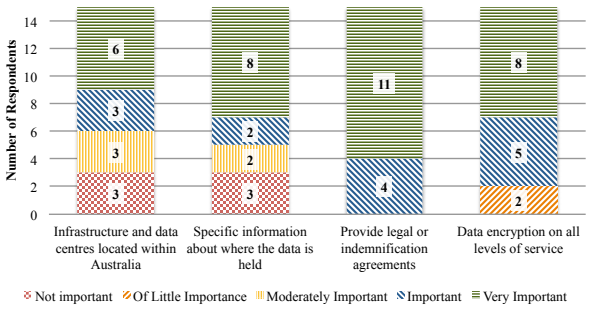

Figure 10: Factors influencing enterprise adoption of cloud computing.

5.5 Customer Orientation

The enterprise survey asked respondents to rate how important they thought various customer-related practices were in their organisations. The findings in Figure 6 (scale of 1=Unimportant to 5=Very important) revealed that businesses place relatively low importance on customers knowing and having control over where their information is stored. Higher importance is placed on informing customers about how their information is collected, used and shared with third parties.

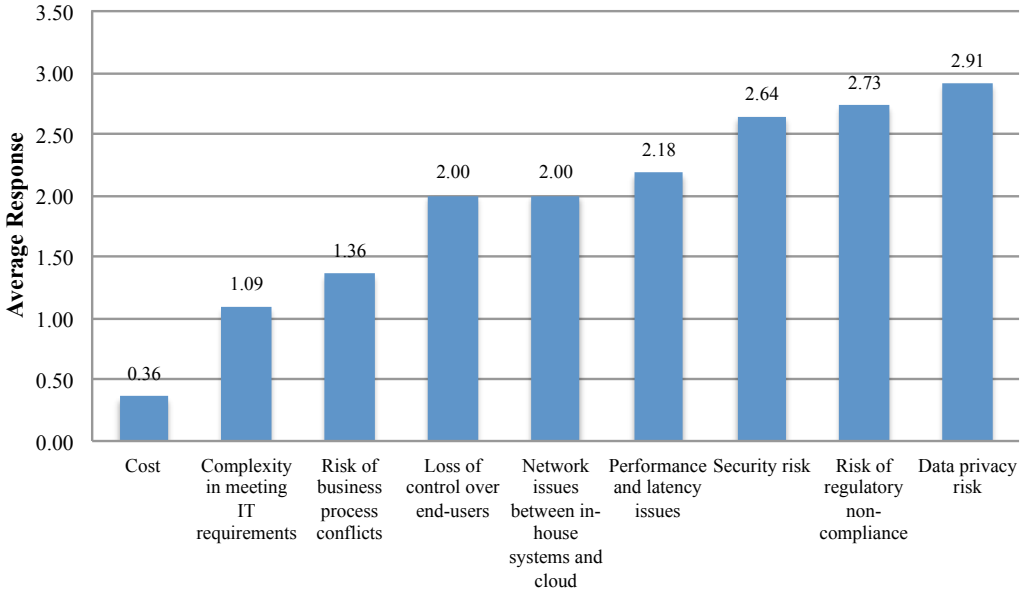

Figure 11: Disadvantages of cloud computing according to enterprises

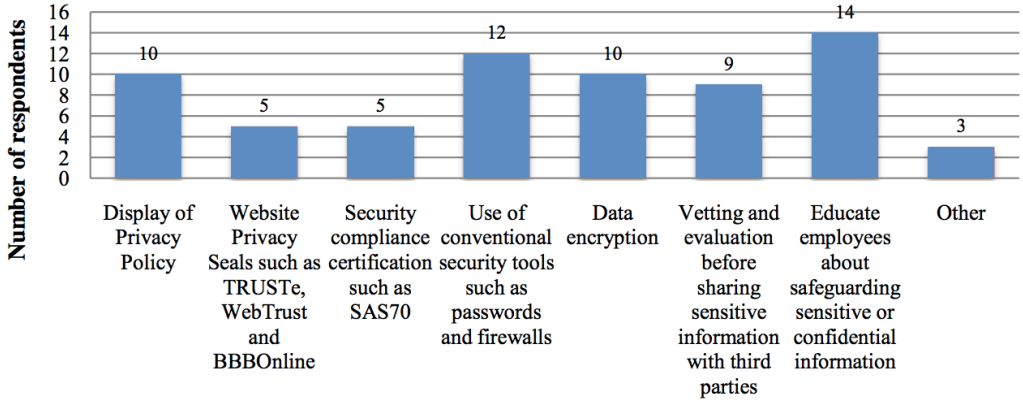

Figure 12: Enterprise methods to protect customer-related information.

5.6 Privacy Protection Methods

The enterprise survey also explored the methods that businesses use to protect customer-related information (Figure 12). 14 of the 15 respondents (93%) surveyed revealed that their organisations trained their employees about proper practices for safeguarding customer information. It was also interesting to find that two-thirds of these organisations (10 out of 15) implement data encryption mechanisms.

5.7 Analysis

Two-thirds of the enterprises surveyed currently employ some form of cloud service, with SaaS being the most widely-used service model. Cloud use among these companies is still in the early stages of adoption and for the most part makes up less than 25% of the organisations' total IT requirements. However more than half the respondents expect the use of cloud services to grow the coming years.

Surprisingly, the majority of respondents stated that the National Broadband Network (NBN) played little importance in their companies' strategic plans for cloud adoption. On the whole, respondents reported that their businesses place relatively low value on customers knowing and having control over where their information is located. Data privacy risk is deemed the biggest disadvantage for enterprises considering cloud computing adoption, followed by the risk of regulatory non-compliance. The main concerns that respondents have with storing or processing customer-related information in the cloud are risks of unauthorised data access and losing control over data location. The availability of legal or indemnification agreements is the most important factor influencing adoption of cloud computing among the enterprise respondents surveyed.

6 Summary and Conclusions

On the whole, this study has demonstrated the ineffectiveness of common privacy protection mechanisms used by companies, such as privacy notices and privacy seals, in communicating a company's privacy practices to end users. Most consumers would not have read the privacy notice before using an Internet service and even in situations when they do pay attention to it, the document may be too verbose and complicated for the common layman to extract any real value from it. Privacy seals on the other hand do not inspire consumer trust and rightly so considering the poor track record of these seals in actually enforcing privacy protection (Gellman 2000).

As past researchers have asserted, the privacy protection afforded by the legal systems of most countries have not kept abreast with the globally distributed nature of Internet technologies (Jaeger et al. 2008). While having data centres located in Australia to cater for domestic cloud computing needs is one pos-

sible solution for transborder data issues, it is not the panacea. Privacy issues such as appropriate collection, use and disclosure of data still exist although the entire cloud is within one and the same jurisdiction (Svantesson & Clarke 2010).

Though it would be ideal for cloud computing providers to deploy encryption for all their products by default, the lack of financial motivation and the performance implications of such a mechanism, it is unlikely that default encryption will become a norm. However, the user's privacy protection could be enhanced with a mechanism to automate greater transparency for the handling of personal information. Such a mechanism would be able to inform individuals where their data is located and where it moves to. On-going notifications of this sort may be beneficial to individuals to keep them informed about the movements of their personal data.

Data privacy in cloud computing is a complex issue that involves many different stakeholders and their contrasting interests. In an ideal world, there would be the perfect balance of technological innovation, commercial interest, consumer interest and information policy. This study strives to contribute to this goal as it provides an overview of the current cloud computing environment in Australia and the data privacy issues that have brought concerns to enterprises and end users in this country. Cloud computing will play an important role in the future of IT, but as this study of user awareness and policy compliance from both enterprise and end user viewpoints has shown, the technology's privacy risks necessitates the push for greater transparency coupled with stronger privacy protection legislations.

References

Amazon (2012*a*), 'Amazon elastic compute cloud (Amazon EC2)'.
URL: *http://aws.amazon.com/ec2/*

Amazon (2012*b*), 'Amazon virtual private cloud (amazon vpc)'.
URL: *http://aws.amazon.com/vpc/*

Armbrust, M., Fox, A., Griffith, R., Joseph, A., Katz, R. & et al., A. K. (2009), Above the clouds: A berkeley view of cloud computing, Technical Report UCB/EECS-2009-28, EECS Department, University of California, Berkeley.

Australian Government (2001), 'Guidelines to the national privacy principles'.
URL: *http://www.privacy.gov.au/materials/*

Australian Government (2010b), 'Privacy law', URL: http://www.privacy.gov.au/law.

Burghardt, T., Böhm, K., Buchmann, E., Kühling, J. & Sivridis, A. (2009), A study on the lack of enforcement of data protection acts, Technical report, Institute for Program Structures and Data Organization (IPD), Karlsruhe Institute of Technology.

Carr, N. (2008), *The big switch: Rewiring the world, from Edison to Google*, WW Norton & Company.

Clarke, R. (2010), Computing clouds on the horizon? benefits and risks from the user's perspective, *in* 'The 23rd Bled eConference eTrust: Implications for the Individual, Enterprises and Society'.

Earp, J. B., Anton, A. I., Aiman-Smith, L. & Stufflebeam, W. H. (2005), 'Examining internet privacy policies within the context of user privacy values', *IEEE Transactions on Engineering Management* **52**(2), 227–237.

Foley, J. (2008), 'Private clouds take shape', *Information Week* .

Gartner (2010), 'Hype cycle for emerging technologies'.

Gellman, R. (2000), 'Truste fails to justify its role as privacy arbiter', *Privacy Law and Policy Reporter* **7**(6).

Gellman, R. (2009), 'Privacy in the clouds: Risks to privacy and confidentiality from cloud computing'.

Google (2009), 'Google App Engine: Country-specific storage', *Google Code* (193).

Hall, M. (2009), 'Pioneers of the private cloud', *Computerworld* **43**(35), 14.

Hutchinson, J. (2010), 'Pendulum swings back toward private cloud: Idc', *Computerworld* .

Jaeger, P. T., Lin, J. & Grimes, J. M. (2008), 'Cloud computing and information policy: Computing in a policy cloud?', *Journal of Information Technology & Politics* **5**(3), 269–283.

Mell, P. & Grance, T. (2009), The NIST definition of cloud computing, Technical report, National Institute of Standards and Technology, Information Technology Laboratory.

Microsoft (2012), 'Windows Azure products'.
URL: *http://www.microsoft.com/windowsazure/*

Milne, G. R. & Culnan, M. J. (2004), 'Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices', *Journal of Interactive Marketing* **18**(3), 15–29.

Mowbray, M. (2009), 'The fog over the grimpen mire: Cloud computing and the law', *Script-ed Journal of Law, Technology and Society* **6**(1).

Neuman, W. L. (2006), *Social Research Methods: Quantitative and Qualitative Approaches*, 6th edn, Pearson Allyn & Bacon.

O'Neill, L. (2010), 'Cloud computing models: Public vs. private vs. hybrid. focus brief'.

Rudraswamy, V. & Vance, D. (2001), 'Transborder data flows: adoption and diffusion of protective legislation in the global electronic commerce environment', *Logistics Information Management* **14**(1/2), 127–136.

Salesforce (2012), 'Salesforce.com platform'.
URL: *http://www.salesforce.com/au/platform/*

SurveyMonkey (2012), 'Survey monkey service'.
URL: *http://www.surveymonkey.com/*

Svantesson, D. & Clarke, R. (2010), 'Privacy and consumer risks in cloud computing', *Computer Law & Security Review* **26**(4), 391–397.

The Gallup Organisation (2008), 'Data protection in the european union – citizens' perceptions'.
URL: *http://ec.europa.eu/public_opinion/*

Vail, M. W., Earp, J. B. & Anton, A. I. (2008), 'An empirical study of consumer perceptions and comprehension of web site privacy policies', *IEEE Transactions on Engineering Management* **55**(3), 442–454.