Privacy and Security in the Cloud: A Review of Guidance and Responses

Edgar A. Whitley
London School of Economics and Political Science
UNITED KINGDOM

Leslie P. Willcocks
London School of Economics and Political Science
UNITED KINGDOM

Will Venters
London School of Economics and Political Science
UNITED KINGDOM

ABSTRACT

Privacy and security issues are frequently presented as major inhibitors of cloud adoption. Some of these are operational issues and others relate to regulatory and compliance requirements that vary by industry and location. There is a growing body of guidance that seeks to clarify the implications of these concerns for various parts of the cloud supply chain. This paper provides a review of the business and legal risks associated with cloud computing and critically reviews the guidance available. It pays particular attention to the implications of the PRISM revelations for the development of a cloud marketplace that aims to keep data private and secure. A number of responses to cloud risks are available, including technological fixes and business responses. Each response has its own costs and requirements in terms of organisational capability and the paper evaluates the various responses that potential cloud adopters can use to manage the risks associated with cloud computing.

INTRODUCTION

Cloud computing can be seen as a service–based perspective on the provision of computing through the exploitation of technical innovations such as virtualization, high–performance networks and data–centre automation (Venters & Whitley, 2012; Willcocks et al., 2014). Academic interest in the topic has mirrored business interest in the opportunities it affords. For example, in 2010, Amazon's annual revenue from cloud services was estimated at between $500m and $700m (The Economist, 2010) and Forrester have predicted a global market for cloud computing worth $61bn for 2012 (Kirsker, 2012). Forrester believe that this will grow to $241bn by 2020 (Dignan, 2011). Finally, a recent study by CEBR (2011) predicts that the adoption of cloud computing has the potential to generate 763 billion euros of cumulative economic benefits over the period 2010–2015 as well as an additional direct and indirect job creation impact of nearly 2.4 million jobs (Centre for Economics and Business Research, 2011).

Despite these economic benefits, there are a number of espoused factors that are currently limiting the take up of cloud computing. Some of the most frequently raised concerns relate to questions of the security and privacy of data held in the cloud (Anthes, 2010; Krutz & Vines,

  ISSN: 1543-5962-Printed Copy ISSN: 1941-6679-On-line Copy

2010; Paquette et al., 2010; Ryan, 2010). For example, a survey with over 1000 respondents undertaken in 2010 found that over 60% of respondents believed that business risks associated with privacy and security were greater for cloud services than traditional data processing. Over 50% reported greater concerns about data being held overseas and over 40% reported enhanced concerns about compliance / regulatory issues (Willcocks et al., 2011a). This level of concerns is echoed in more recent surveys (e.g. Computer Weekly, 2013).

In some cases these concerns were actually preventing the adoption of cloud services (Everest Group, 2013). In other cases, security and privacy increased the costs of adopting cloud by requiring increased diligence in assessing cloud suppliers (Seddon & Currie, 2013). Finally, there is also the perspective, that these concerns can be exaggerated by IT departments who are reluctant to cede further control over, or out of the IT function—departments, perhaps, that have learned their own lessons from the outsourcing revolution.

The purpose of this paper is to review and contextualise the nature of these concerns, to evaluate the guidance that is available about them and to assess the potential legal, technological and business responses to them. Thus the paper's purposes are to describe the main concepts relating to privacy and security as they apply to cloud computing, relating exemplars of the existing guidance to these concepts and hence enabling new concerns and forms of guidance to be understood in relation to the existing available literature (Webster & Watson, 2002).

In particular, the paper suggests that the privacy and security concerns that can arise when moving to the cloud are best understood from a risk–based perspective. This allows all parties to differentiate between operational risks and regulatory and compliance risks. The review also enables them to better appreciate which risks can be mitigated by an effective cloud sourcing strategy, which can be addressed by cloud providers and which are the unavoidable but possibly manageable risks of doing business.

The next section therefore seeks to understand the landscape of privacy and security concerns by reviewing the key business and legal / compliance issues that cloud computing raises. In order to ground these concerns, the paper focuses on the requirements of UK data protection legislation that are driven by the EU Data Protection Directive. It contrasts them with associated regulatory requirements in other jurisdictions, particularly the United States. This is followed by a section that summarises some of the most recent guidance on privacy and security issues in the cloud. This is followed a section that considers specific technological and business responses to the privacy and security challenges. The paper ends with a summary of the likely future direction of privacy and security in the cloud.

UNDERSTANDING THE LANDSCAPE OF PRIVACY AND SECURITY CONCERNS

Some concerns with the privacy and security of cloud computing are based on business considerations, others are grounded in specific legal and compliance requirements based on industry or geographical requirements. Whilst some of these concerns are being reviewed in the academic literature (particularly the law literature) other issues are currently grounded in practice, practitioner reports and case studies and are only slowly finding their way into the

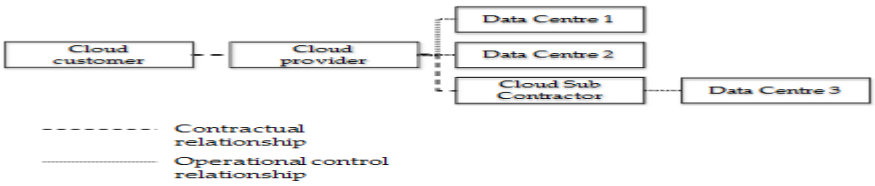
  ISSN: 1543-5962-Printed Copy ISSN: 1941-6679-On-line Copy

academic literature (Swanson & Ramiller, 2004). This section therefore reviews these diverse concerns that emerge from both theory and practice.

The Business Basis of Privacy and Security Concerns

Many of the privacy and security concerns raised in the context of cloud are a direct consequence of the nature of the cloud proposition, particularly in the early years of cloud adoption where the benefits have been invariably presented in terms of cost reduction. According to this view, cloud computing transforms the nature of IT provision from specific, internally hosted and managed IT resources to commodity hardware and software platforms hosted outside the organizational boundary (Willcocks et al., 2014). In order to provide the lowest cost offering, cloud providers may switch the (cloud) customer's data and processes from one hardware instantiation to another and it is precisely this switching that raises some of the privacy and security issues. Thus, in Figure 1 the Cloud Customer has a contract with the Cloud Provider for the provision of cloud services. This Cloud Provider runs two data centres (Data Centre 1 and Data Centre 2). In addition, in order to manage loading issues, the cloud provider also has a contractual relationship with a Cloud Sub Contractor which runs Data Centre 3. Thus, in this simplified scenario the cloud customer's data might be located or replicated in Data Centre 1, Data Centre 2 or Data Centre 3.

Figure 1: Key cloud actors and relationships.



From a security perspective, if critical data and processes are hosted on various 'random' hardware instantiations, significant risks are introduced for the cloud customer. Some of these risks have been discussed in the academic literature, whilst others have only been raised in practitioner forums. In order to combine insights from the academic literature and the 'grey literature', these issues are presented as a series of "questions". The first set of questions relate to concerns that cloud customers are asking. Typically these cloud customers are enterprises using cloud services but equally could be members of the public using cloud technology directly.

- How can the customer be sure that their data and processes are not accessible to staff working for the cloud service provider or to other customers running their services on the same hardware environment etc.?
- How can the customer be sure that, when the use of the hardware comes to an end (either when demand patterns change and cloud hardware is decommissioned or when the cloud provider relocates the customer's services to other, cheaper computing resources) any data stored on that hardware is irreversibly removed? Alternatively, if there are legal obligations on a company to retain data, what

ISSN: 1543-5962-Printed Copy ISSN: 1941-6679-On-line Copy

guarantees are there that the data will remain available for the retention period (often measured in years)?

- If the cloud provider is hosting mission critical services, how can the customer be sure that the cloud provider's disaster recovery plans are effective?
- Is there a risk that despite claims that the choice of cloud provider is open and based on commodity hardware that there will not be attempts to lock–in the customer—either by using slightly non–standard hardware configurations or because of the sheer impracticality of transferring data and processes to another provider at contract renewal time?
- What are the risks of using a cloud data–centre that is co–hosting many companies' data? "Sharing" a cloud provider with other brands can have unintended consequences that cannot be easily calculated. For example, one unintended consequence of Amazon and DynDNS hosting WikiLeaks was that these services were targeted by hackers with consequent adverse effects on other users of their services.

Cloud providers similarly face their own version of these challenges:

- What levels of staff accreditation need to be implemented to demonstrate to customers that their staff will not misuse the data held on their cloud hardware? Would offering on–site security inspections reassure customers about security concerns or would the costs of doing so be prohibitive?
- What forms of data–wiping need to be offered to customers? How computationally expensive are these processes and how does this affect the cost of the cloud service? Would it be appropriate to offer these services at a premium or is it best to develop an architecture that offers this functionality to all users?
- What disaster recovery mechanisms should the provider have in place or should they limit the service they offer to simple hardware platforms and put the responsibility for disaster recovery on the customer? How will the provider's reputation be affected by a major outage?
- How does the cloud provider balance between offering commodity products sold on the basis of price and service quality and offering distinctive capabilities which might raise customer concerns about lock in?

The Legal Basis of Privacy Concerns

Whilst many of the security concerns outlined above are driven by business needs (of the customer and of the cloud providers), concerns over the privacy of personal data are often directly linked to specific legal requirements regarding the processing of personal data. For example, the EU data protection directive (translated into specific national legislation, such as the UK's Data Protection Act) places specific obligations on companies handling personal data.

In the UK *personal data* is defined as data which relate to a living individual who can be identified from those data, or from those data and other information which is in the possession of, or is likely to come into the possession of, the company and includes any expression of

opinion about the individual and any indication of the intentions in respect of the individual (Information Commissioner's Office, 2013).

Similarly, the UK Data Protection Act defines the *data controller* as the entity who decides how and why data is processed. Most frequently the *data controller* is an enterprise that is processing the data about *data subjects* (the people whose data is being processed) but the *data controller* could also be an individual member of the public. The actual processing of the data may be handled by another party. The *data processor* processes the data on behalf of the *data controller*. In many situations the *data controller* and the *data processor* may be the same organisation but, with the growth of cloud and outsourced services, the data processor is increasingly not part of the same organization as the data controller. Regardless of the relationship between the data controller and data processor it is the data controller who remains responsible for ensuring that "their" processing complies with the Act, whether they do it in–house or engage an external data processor. Outsourced data processors are therefore not directly subject to the Act. Where roles and responsibilities are unclear, the Information Commissioner's Office states that they will need to be clarified to ensure that personal data is processed in accordance with the data protection principles adding that for these reasons organisations should choose data processors carefully and have in place effective means of monitoring, reviewing and auditing their processing (Information Commissioner's Office, 2013).

Although the Data Protection Act applies to all personal data, extra requirements apply when handling "sensitive personal data" which is defined as data relating to the racial or ethnic origin of the individual, his political opinions, his religious beliefs or other beliefs of a similar nature, whether he is a member of a trade union, his physical or mental health or condition, his sexual life, the commission or alleged commission by him of any offence, or any proceedings for any offence committed or alleged to have been committed by him. In addition, certain regulated industries impose their own best practice requirements in relation to the handling of data related to their industry, for example, the Payment Card Industry Data Security Standards (PCI–DSS) which provide an actionable framework for developing a robust payment card data security process requirements that apply (PCI, 2013).

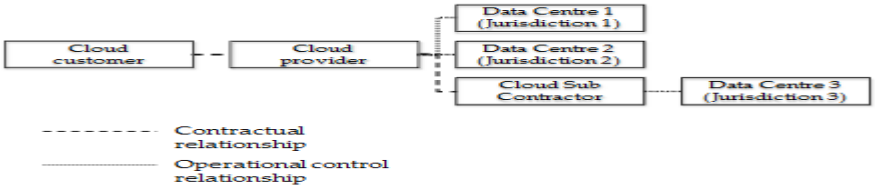
The relationship between privacy and security can be seen in the seventh data protection principle of the UK Data Protection Act. This provides that:

> Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data (Information Commissioner's Office, 2012b).

The eighth data protection principle provides that:

> Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data (Information Commissioner's Office, 2012b).

Figure 2: Key actors, relationships and jurisdictions.



It is the combination of these requirements that becomes important in the context of cloud computing. To represent this,

Figure 2 updates Figure 1 to include the jurisdiction where each of the three data centres is located. In addition, the paper adopts the terminology whereby the cloud customer in

Figure 2 is a *data controller* as defined by the Data Protection Act and the cloud provider is the *data processor*. In the case where the cloud provider is offering software–as–a–service, rather than infrastructures or platforms as a service, it is possible that they might actually be considered as joint data controllers rather than data processors (Article 29 Data protection working party, 2010).

Thus, there is an obligation on a cloud customer, who uses a cloud provider to act as the data processor, to ensure personal data is not being transferred outside the European Economic Area unless that country or territory ensures an adequate level of data protection rights. Only a few countries are judged by the EU to offer an "adequate level of protection" including Switzerland, Argentinia and Canada (EU, 2013). Thus, if Data Centre 3 is not in a territory that offers an adequate level of data protection rights, the Data Protection Act prevents an EU cloud customer from transferring the data to Data Centre 3 unless the cloud customer obtains the permission of every person whose data would be transferred to that Data Centre. Another potential solution is to utilise Safe Harbour type provisions, where cloud providers self–assert that they are in compliance with EU requirements. When coupled with Binding Corporate Rules, these mechanisms might offer sufficient mitigation of data protection concerns (King & Raja, 2013).

In the absence of one of these solutions, cloud customers might only be able to use a cloud provider with a data centre in the EU and only then if the cloud provider can ensure that the data is only held there. For example, although Amazon EC2 offers a choice of location for some of its cloud services for customers to use: US East Coast, US West Coast, Asia and Ireland, an EU based customer may only be able to use the Irish data centre. Such restrictions may limit operational benefits that could be offered by the cloud provider including data replication that might provide a cheaper service at a lower latency rate or an ability to reallocate resources quickly if one data centre suffers a particular outage (Esayas, 2012).

ISSN: 1543-5962-Printed Copy ISSN: 1941-6679-On-line Copy

In other cases, the cloud provider may be unable to provide this information / guarantee that the personal data is not held on cloud hardware that is not located within the EEA or in a suitably accredited location.

Failure to address privacy and data protection concerns adequately can result in the cancellation of cloud services. For example, in June 2013 the Swedish Data Inspection Board issued a decision that prohibits the nation's public sector bodies from using Google's cloud based apps including calendar, email and data processing functions (Davies, 2013). The ruling was based on a risk assessment by the Board and is based on problems with the contracts offered by Google. According to the Swedes, the contract gives Google too much covert discretion over how data can be used and left public sector customers unable to ensure that data protection rights are protected. Several examples of the kinds of deficiencies in the contract were noted including uncertainty over how data may be mined or processed by Google and a lack of knowledge about which subcontractors may be involved in the processing. The assessment also concluded that there was no certainty about if or when data would be deleted after expiration of the contract (Davies, 2013). In 2012 the Norwegian data protection authority insisted on contractual adjustments for similar reasons before they would permit Norwegian local authorities to use Google apps (Davies, 2012).

In contrast to the EU approach which sees privacy as a fundamental human right the US approach tends to focus on preventing specific, serious risks of economic harm that may result from misuses of sensitive personal data (King & Raja, 2013). Thus, there are categories of consumer data that have strong information privacy requirements. These affect websites that collect information on children under the age of thirteen years, financial institutions and credit reporting agencies and health care providers. For example, in the health sector, the Office for Civil Rights enforces the Health Information Portability and Accountability Act (HIPAA) which places specific obligations on health care providers and imposes security standards for the security of electronic protected health information (Seddon & Currie, 2013).

In each case, the privacy requirements exist because there is deemed to be a clear link to potential economic harm arising from the misuse of this data (King & Raja, 2013). One consequence of these very different approaches to privacy protection is the lack of universally applicable responses to the privacy concerns.

GUIDANCE AND ADVICE ON PRIVACY AND SECURITY ISSUES

At first sight, these privacy and security concerns might appear to be insurmountable and make cloud computing an impractical option for most enterprises. However, numerous bodies have issued advice and guidance on these issues. In addition to conventional engagement with the academic literature, the authors are also immersed in a range of academic, civil society and practitioner networks. This immersion includes subscribing to relevant mailing lists, giving presentations for practitioners and participating in policy debates around privacy and security with government and industry. These diverse networks provide two useful functions for this review: first, they are useful gateways to the relevant grey literature; second, they provide frank assessments of the usefulness or not of particular forms of guidance. For example, the authors first became aware of the Sopot memorandum (described below) through participation in a

practitioner network where a trusted colleague endorsed the utility of the document. Similarly, they received details of the European Parliament report through a civil society discussion list where the expertise of the report's authors was widely acknowledged. These networks include notifications of other forms of guidance, often accompanied by "less supportive" assessments of the utility of the guidance. This paper has therefore drawn on these assessments in determining which forms of guidance to focus on in this review.

The European Commission has a new strategy for unleashing the potential of cloud computing in Europe which it claims will result in a net gain of 2.5 million new European jobs and an annual boost of €160 billion to EU GDP by 2020 (European Commission, 2012). According to the EU, the strategy is designed to speed up and increase the use of cloud computing and key actions of the strategy include developing standards on issues including data portability and reversibility, EU–wide certification schemes for trustworthy cloud providers and the development of model 'safe and fair' terms for cloud contracts. Similarly, the US and South Korean governments are promoting cloud usage within government services, to both improve the quality and innovation in services provided to their citizens but also to help develop the cloud competences more generally (Esayas, 2012).

The first outputs from the EU work will be 'safe and fair' contract terms (Kroes, 2013). These are needed, according to Neelie Kroes, Vice–president of the European Commission, because "people don't always understand the terms in their contract: what they're paying for and what they can expect". She particularly highlighted the concerns of small and medium enterprises:

> Who might hesitate to use the cloud because of fears that they will not meet their legal obligations, or who might be worried that they get locked in or stranded by changes of technology or service by cloud providers. They don't want the risk of getting mired in foreign court cases in foreign languages; nor of exposing the data which may be their business's life blood to security risks or breaches. And they cannot afford costly legal fees to figure all this out case by case (Kroes, 2013).

More specific guidance comes from detailed reports such as the 'Sopot memorandum' produced by Data Protection Commissioners from different countries to improve privacy and data protection in telecommunications and media (International Working Group on Data Protection in Telecommunications, 2012). The guidance notes that, at present, with the increased globalization of data processing (perhaps, more accurately the use of "multiple locales (data centres) distributed across different jurisdictions and different private operators" (European Parliament, 2012)) there is a lack of transparency about cloud service provider processes, procedures and practices, including whether or not cloud service providers sub–contract any of the processing and if so, what their respective processes, procedures and practices are. They note that this lack of transparency makes it difficult to conduct a proper risk assessment as well as increase the difficulty of enforcing rules regarding data protection (International Working Group on Data Protection in Telecommunications, 2012).

Important consequences of this lack of transparency include data being transferred to jurisdictions that do not provide adequate data protection, acts in violation of laws and principles for privacy and data protection and the data controller accepting standard terms and conditions

  ISSN: 1543-5962-Printed Copy ISSN: 1941-6679-On-line Copy

that give the cloud service provider too much leeway, including the possibility that the cloud service provider may process data in a way that contradicts the controller's instructions (International Working Group on Data Protection in Telecommunications, 2012).

The Working Group recommended that the adoption of cloud computing should not lead to a lowering of data protection standards as compared with conventional data processing; that data controllers need to carry out the necessary privacy impact and risk assessments (if necessary, by using trusted third parties) prior to embarking on cloud projects. They also recommended that cloud service providers further develop their practices in order to offer greater transparency, security, accountability and trust in cloud solutions in particular regarding information on potential data breaches and more balanced contractual clauses to promote data portability and data control by cloud users (International Working Group on Data Protection in Telecommunications, 2012).

In a similar manner, the UK Information Commissioner's Office also issued guidance on cloud computing (Information Commissioner's Office, 2012a). This noted that by processing data in the cloud "an organization may encounter risks to data protection that they were previously unaware of" and suggested that data controllers take time to understand the data protection risks that cloud computing presents. In addition to the points noted above, the ICO's guidance points out that it may not be necessary to move all data and processing to the cloud and that many data protection risks may be mitigated by separating out the processing of personal data from that of non–personal data. The personal data could be processed internally and all other data processed in the cloud. This avoids the legal uncertainties associated with the cloud based data.

It should be noted, however, that processing data in the cloud also often results in the creation of audit records and other metadata. If this data is associated with particular customers then this metadata is itself personal data (as it can be associated with an identifiable individual) and is subject to the provisions of the Data Protection Act.

Whilst much of this guidance is written from the perspective of allowing / encouraging business to keep using cloud services, there is some guidance that is presented firmly from the perspective of the citizen whose personal data might be held and processed in the cloud. For example, in 2012 the European Parliament issued a report that explicitly sought to protect privacy in the cloud (European Parliament, 2012) (rather than just ensuring compliance with existing data protection legislation). The report suggested that the challenge of privacy in the cloud has been underestimated if not ignored completely and suggested that the main concern for private citizens is not so much the possible increase in "cyber" fraud or crime but is instead "the loss of control over one's data" (European Parliament, 2012). The report argued that from this perspective the most disruptive feature of cloud computing has nothing to do with technical or business innovation but is instead where "it breaks away from the forty–year–old legal model for international data transfers" (European Parliament, 2012). As a result, the report argued that consumers' fundamental rights, as embodied in data protection, are lost in a complex mesh of contracts and service level agreements with the private sector companies that are cloud providers.

Further effects on the legal rights of citizens regarding their data arise in the context of "exceptional measures" taken in the name of security and counter–terrorism. As the report noted, this is particularly significant in the US context where both the Patriot Act and the US Foreign Intelligence Surveillance Amendment Act (FISAA) 2008. The Patriot Act was signed into law in 2001 and included amendments to federal statutes that regulated wiretaps and access to stored electronic communications. This was done in order to broaden law enforcement's access to electronic records (King & Raja, 2013). A particular concern related to the scope of the provisions of the Patriot Act which offered protections for US citizens but not others (Balboni & Pelino, 2013).

That is, jurisdiction matters (Goldsmith & Wu, 2006). The legal environment that applies to the cloud providers (and particularly the regulations that apply to the location where they host their infrastructure) can limit any protections that citizens may expect with regard to the processing of their data. For example, a number of companies claim that US "Safe harbour" certification legalises transfers of EU data into US cloud (European Parliament, 2012). However, according to the European Parliament report, §1881a of FISAA created mass–surveillance specifically targeted at the data of non–US persons located outside the US (as would apply to cloud computing). The law was passed in the aftermath of allegations of "warrantless wiretapping" of US citizens where accounts emerged in 2005 that, in violation of strict constitutional protections, surveillance of internet and telephone communications of US citizens (and legal residents) had been conducted. After various legal measures and cases reviewing the relationship between US citizens and others, Congress enacted FISAA in 2008.

The use of these types of powers re–entered the public imagination in May 2013 when whistle blower Edward Snowden revealed that the US PRISM programme had been surreptitiously surveying the communications data of US and non–US citizens including national leaders such as German chancellor Angela Merkel (BBC News, 2013), with allegations that the UK government was also monitoring this kind of data (The Guardian, 2013). Technology companies and cloud providers like Google and Yahoo noted that they were not even allowed to disclose the information they were forced to disclose to the US government. This highlights the risk that cloud providers may be forced to disclose their clients' data and may not even be allowed to inform the clients that this has taken place.

In a briefing note to the EU Directorate General for Internal Policies, Bowden (2013) reassesses the recommendations in the European Parliament report on cybercrime and privacy in the cloud (European Parliament, 2012) in the light of the PRISM revelations. He recommends that prominent notices should be displayed by every US web site offering services in the EU. In particular, he argues that "users should be made aware that the data may be subject to surveillance (under FISA 702) by the US government for any purpose which furthers US foreign policy". He further argues that since the other existing mechanisms for data export (such as model contracts, Safe Harbour) are not protective against FISA or PATRIOT, they should be revoked and re–negotiated. Finally, he recommends strong support for a European cloud industry that would enable "durable data sovereignty" within Europe (Section 3.1). Other reports have made similar recommendations (e.g. Bigo et al., 2013) and the ideas appear to have gained traction in the negotiations around the new General Data Protection Regulation (Brandenburg, 2013).

ISSN: 1543-5962-Printed Copy ISSN: 1941-6679-On-line Copy

RESPONDING TO PRIVACY AND SECURITY CONCERNS

Given the range of concerns faced by corporations moving to the cloud, it is unsurprising that a range of responses are available to the organization. In addition to the guidance outlined above, there are further options that organizations can use. The specific configuration of options will be determined, to a large extent, by the maturity and evolution of the marketplace and institutional actors (Kshetri, 2013) as well as the internal capabilities of cloud customers and providers. Some options are technologically driven whilst others are business choices that will reflect the risk profile of the enterprise.

Technological Responses

There are a range of technological responses to privacy and security concerns (Pearson, 2013). One important development highlighted in the recent EU Data Protection Regulation (European Commission, 2012) is the concept of privacy–by–design and, similarly, security–by–design (Oetzel & Spiekermann, 2013). It is widely recognised that bolting privacy (and security) functionality on top of an existing system is frequently ineffective and always more costly than designing systems where these capabilities are built in from the start (Information Commissioner's Office, 2008). Thus, enterprises seeking to use cloud services and cloud providers hoping to increase their market share at a time of low trust in cloud computing services might adopt privacy–by–design style thinking when developing their applications and services.

One example of such an approach which seeks to address the problem of concerns about third parties gaining unlawful access to data held on cloud servers is to build in cryptographic techniques into the cloud infrastructure (Pearson et al., 2011). These techniques encrypt data (both personal data and enterprise data) as it moves to and from the cloud in much the same way as it is now possible encrypt the personal data held on smartphones and tablets (Ryan, 2013). These encryption services might be administered by the cloud customer, or might be offered as a value–added service by the cloud provider. In each case, nevertheless, there can be significant computational costs associated with the encryption / decryption process. In addition, there may be liability issues associated with encryption services offered by the cloud provider: if they have provided this customer with the decryption keys, what assurances does the customer have that they haven't shared the same keys with other parties?

The complexities and costs of managing the various encryption keys, issuing replacement keys, authorising and de–authorising key users, are well understood in mainstream computing environments and are increasingly being appreciated in the cloud context. As with many of these responses, their successful implementation will depend to a large extent on the internal capabilities and organizational learning of all parties in the cloud supply chain (Willcocks et al., 2011b).

A related technological response is to have strictly enforced access controls associated with cloud data and processing. These access control mechanisms help ensure that only suitably authorised role holders are able to gain access to or modify data and processes in the cloud (Noureddine & Bashroush, 2013). When successfully implemented, these techniques open up

ISSN: 1543-5962-Printed Copy ISSN: 1941-6679-On-line Copy

the possibility for innovative co–operation along an entire production supply chain. For example, rather than having production and distribution data held by one of the hubs in the supply chain, all this data could be held in the cloud with each part of the supply chain having (suitably controlled) access to that part of the data that they need for their own stage of the production process. Again, there is growing evidence of the complexity of managing this task within modern enterprises where role definitions are increasingly fluid (JISC, 2010; Whitley et al., 2014).

Another technological mitigation involves the choice of cloud model that the enterprise adopts. For example, in some circumstances an enterprise might benefit from using a "private cloud" rather than a "public cloud". That is, it creates its own data centre within the organization's boundaries. This data centre can still offer the benefits of scalability and rapid provisioning of computing resources, as well as the cost reductions associated with consolidated data centres, but without running the risks of external organizations having access to their data.

Another alternative, suggested above, is a hybrid cloud model whereby some data (typically the data that needs to be protected in terms of data protection legislation) is kept 'in house' whilst less sensitive (or mission critical) data is held in a public cloud. In practice, however, the boundaries between what should be kept in house and what could be held in the public cloud are not clear cut. For example, office productivity tools like email and document processing can frequently be provided at lower cost in the public cloud (e.g. Google Apps) but may, in fact, contain personal data or commercially sensitive information that the enterprise deems should be kept 'in house'.

Cloud providers are also seeking to signal their security credentials transparently. For example, Amazon has moved to acquire existing security standards (e.g. ISO 27001) for its cloud services.

Business Responses

In addition to technological responses to cloud privacy and security concerns, there are a range of business responses that can be adopted. Assuming that the (cloud customer) enterprise has actually read and understood the terms of the contact offered by the cloud provider, the enterprise could use its risk profile to determine whether it is prepared to accept those terms or offer a requirement for counter–terms. In some cases of a 'single size for all' type contract (such as those offered by Google Apps to local authorities in Scandinavia) the opportunity for negotiation may be limited. In other cases, on seeing a pattern of specific requests for certain services or warranties, the innovative cloud provider may offer a range of different pricing options for customers to choose amongst, thus segmenting the market place on the basis of price and (additional) services offered.

For example, a cloud provider might offer potential customers the opportunity to do their own penetration testing of the cloud provider or allow them to inspect the physical security of the data centre or the vetting process for staffing hire. In other cases, third party certification agencies might be prepared to assure the enhanced security and privacy claims made by the cloud provider. In each of these cases, however, a cloud customer needs to be aware of the 'Winner's Curse' phenomenon (Kern et al., 2002). This phenomenon arises when, for example, an initially

  ISSN: 1543-5962-Printed Copy ISSN: 1941-6679-On-line Copy

successful cloud provider who gains customers by offering higher levels of service loses that capability as it becomes "too" successful and is unable to hire or retain key staff or expand its hardware capabilities reliably.

Another response involves the close monitoring of service level agreements (SLAs) to ensure that the cloud provider is actually providing the level of service that they had initially promised (Willcocks et al., 2011b). Achieving this requires the development of in–house contract monitoring capabilities. It also, of course, involves ensuring that the original SLA was read and understood. In the case of commodified cloud resources, if the SLA is standard for that market segment but doesn't quite match the customer's needs, the cloud customer must make a risk–based assessment about whether to accept a contract with an SLA that is an imperfect match for their requirements.

Another consideration, particularly at the commodity end of cloud SLAs, relates to what happens if the promised service levels are not met. This is where the enterprise's real understanding of its cloud computing becomes paramount. The failure of a cloud service that allows customers to locate their nearest store for twenty four hours is likely to cause fewer problems for a retailer than the failure of its order processing system for 24 minutes. In the case of a failure to meet agreed service levels (and this might only be spotted by active contract monitoring by the customer), then the terms of the contract need to specify the compensation. In many cases this will be limited to refunding the usage fee for the period of interruption which may only be a few pounds. Close reading of the contract / service level agreement will reveal what duties the cloud provider agrees to undertake and what duties it won't. For example, following a failure with Amazon's cloud services in 2011, many of Amazon's customers 'discovered' that customers who launch server instances in different Availability Zones can "protect [their] applications from failure of a single location" (Wang, 2011). That is, Amazon customers cannot depend on having multiple "Availability Zones" within a specific region as insurance against system downtime (Wang, 2011).

Given the uncertainty about effectiveness of SLAs and the potential costs of monitoring performance, some businesses take a very different approach to managing their cloud risk profiles. That is, rather than closely monitoring the SLAs they have with their cloud providers, they mitigate their risks by drawing on a broad pool of potential cloud providers. If one cloud provider appears to be performing at a substandard level, they simply reduce their usage of that service and switch on alternative cloud providers.

Finally, it should be recognised that although cloud services may change the security risk profile (Anthes, 2010) cloud providers may also be better able to manage security, respond to distributed attacks and invest in sophisticated security hardware and software; facilities that are normally unavailable to all but the largest enterprises. Indeed cloud providers may be able to spot unusual activity, which the individual companies would be unable to identify, by using security analytics to identify unusual behaviour patterns among pools of similar enterprises.

ISSN: 1543-5962-Printed Copy ISSN: 1941-6679-On-line Copy

CONCLUSIONS

There is increasing legislation in the security and privacy areas, generally and also in regard to cloud and legislatures are increasingly trying to catch up with the implications of internet–based technologies and put in place controls and associated penalties for non–compliance with these controls. The ongoing EU discussions about the new General Data Protection Regulation exemplify this point. As noted above, events such as the PRISM revelations can add further perturbations to the regulatory environment. This has an impact on cloud clients and service suppliers alike.

At first sight developments in legislation, guidelines and codes of practice on these privacy and security concerns threaten to make cloud an unattractive option for many as there is an increasing burden of regulation to comply with. However, there are a range of initiatives by regulatory bodies offering guidance and advice. In the EU, the first outputs from this work are the 'safe and fair' contract terms. More specific guidance comes from detailed reports such as the 'Sopot memorandum' produced by Data Protection Commissioners from different countries to improve privacy and data protection in telecommunications and media. Similarly, the UK Information Commissioner's Office also issued guidance on cloud computing to help businesses. Other initiatives focus on the citizen perspectives and emphasize how important jurisdictional issues can be, particularly in relation to privacy concerns.

Faced with these complexities, the paper presented a number of practical technological and business responses to security and privacy concerns arising when moving to the cloud.

REFERENCES

(all URLs valid as at 13 November 2013)

Anthes, G. (2010). Security in the Cloud. *Communications of the ACM,* 53(11), 16-18.

Article 29 Data protection working party (2010). Opinion 1/2010 on the concepts of "controller" and "processor" *WP, 169* (16 February 2010) Archived at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf

Balboni, P., & Pelino, E. (2013). Law Enforcement Agencies' activities in the cloud environment: a European legal perspective. *Information and Communications Technology Law,* 22(2), 165-190.

BBC News (2013). 'US spied on Merkel since 2002' (27 October) Archived at http://www.bbc.co.uk/news/world-europe-24690372

Bigo, D., Carrera, S., Hernanz, N., Jeandesboz, J., Parkin, J., Ragazzi, F., & Scherrer, A. (2013) Mass Surveillance of Personal Data by EU Member States and its Compatibility with EU Law (November) Archived at http://www.ceps.eu/book/mass-surveillance-personal-data-eu-member-states-and-its-compatibility-eu-law

Bowden, C. (2013). The US National Security Agency (NSA) surveillance programmes (PRISM) and Foreign Intelligence Surveillance Act (FISA) activities and their impact on EU citizens' fundamental rights *Directorate General for internal policies: Policy Department C: Citizen's rights and constitutional affairs* Archived at http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/briefingnote_/briefingnote_en.pdf

Brandenburg, A. (2013). EU Parliament's LIBE Committee vote on General Data Protection Regulation paves way for inter-institutional negotiations on new data protection rules in Europe (24 October) Archived at http://blogs.olswang.com/datonomy/2013/10/24/eu-parliaments-libe-committee-vote-on-general-data-protection-regulation-paves-way-for-inter-institutional-negotiations-on-new-data-protection-rules-in-europe/

Centre for Economics and Business Research (2011). The Cloud Dividend – Part Two *CEBR/EMC* Archived at http://www.cebr.com/reports/economic-impact-of-cloud-computing-2/

Computer Weekly (2013). Taking the pulse of the cloud computing market (17 July) Archived at http://www.computerweekly.com

Davies, S. (2012). Why Norway's rigorous stance on Cloud computing highlights the primacy of strong privacy policies (13 June) Archived at http://www.privacysurgeon.org/blog/incision/why-norways-rigorous-stance-on-cloud-computing-highlights-the-crucial-importance-of-strong-privacy-policies/

Davies, S. (2013). Sweden's data protection Authority bans Google cloud services over privacy concerns (13 June) Archived at http://www.privacysurgeon.org/blog/incision/swedens-data-protection-authority-bans-google-apps/

Dignan, L. (2011). Cloud Computing Market: $241 billion by 2020 (22nd April) Archived at http://www.zdnet.com/blog/btl/cloud-computing-market-241-billion-in-2020/47702

Esayas, S. Y. (2012). A walk in to the cloud and cloudy it remains: The challenges and prospects of 'processing' and 'transferring' personal data. *Computer Law & Security Review*, 28(6), 662-678.

EU (2013). Commission decisions on the adequacy of the protection of personal data in third countries Archived at http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm

European Commission. (2012). Digital agenda: New strategy to drive European business and government productivity via cloud computing (27 September) Archived at http://europa.eu/rapid/press-release_IP-12-1025_en.htm

European Parliament. (2012). Fighting cyber crime and protecting privacy in the cloud *Directorate General for Internal Policies; Policy Department C: Citizens' rights and*

constitutional affairs (October) Archived at http://www.europarl.europa.eu/committees/en/studiesdownload.html?languageDocument=EN&file=79050

Everest Group (2013). Enterprise Cloud Adoption Survey – 2013 (March)

Goldsmith, J., & Wu, T. (2006). *Who controls the internet? Illusions of a borderless world.* Oxford University Press, Oxford.

Information Commissioner's Office. (2008). Privacy by design Archived at http://www.ico.org.uk/for_organisations/data_protection/topic_guides/~/media/documents/pdb_report_html/PRIVACY_BY_DESIGN_REPORT_V2.ashx

Information Commissioner's Office. (2012a). Guidance on the use of cloud computing (10 February) Archived at http://www.ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Practical_application/cloud_computing_guidance_for_organisations.ashx

Information Commissioner's Office. (2012b). Outsourcing: A guide for small and medium-sized businesses Archived at http://www.ico.org.uk/for_organisations/data_protection/the_guide/~/media/documents/library/Data_Protection/Detailed_specialist_guides/outsourcing_guide_for_smes.ashx

Information Commissioner's Office.(2013). Key definitions for the Data Protection Act Archived at http://www.ico.org.uk/for_organisations/data_protection/the_guide/key_definitions

International Working Group on Data Protection in Telecommunications. (2012). 'Sopot memorandum' Working Paper on Cloud Computing - Privacy and data protection issues (24 April) Archived at http://germanitlaw.com/wp-content/uploads/2012/04/Sopot-Memorandum1.pdf

JISC (2010). Identity management toolkit. (30 June) Archived at http://www.jisc.ac.uk/whatwedo/programmes/aim/idmtoolkit.aspx

Kern, T., Willcocks, L. P., & Van Heck, E. (2002). The winner's curse in IT outsourcing: Strategies for avoiding relational trauma. *California Management Review*, 44(2), 47-69.

King, N. J., & Raja, V. T. (2013). What Do They Really Know About Me in the Cloud? A Comparative Law Perspective on Protecting Privacy and Security of Sensitive Consumer Data. *American Business Law Journal*, 50(2), 413-482.

Kirsker, H. (2012). 10 Cloud Predictions for 2012 *Forrester.com* Archived at http://blogs.forrester.com/holger_kisker/11-12-13-10_cloud_predictions_for_2012

Kroes, N. (2013). A step forward for cloud computing – safe and fair contract terms (21 June) Archived at http://blogs.ec.europa.eu/neelie-kroes/cloud-contract-term/

Krutz, R. L., & Vines, R. D. (2010). *Cloud security: a comprehensive guide to secure cloud computing.* Wiley, Indianapolis, IN.

Kshetri, N. (2013). Privacy and security issues in cloud computing: The role of institutions and institutional evolution. *Telecommunications Policy,* 37(4-5), 372-386.

Noureddine, M., & Bashroush, R. (2013). An authentication model towards cloud federation in the enterprise. *The Journal of Systems and Software*, 86(9), 2269-2275.

Oetzel, M. C., & Spiekermann, S. (2013). A systematic methodology for privacy impact assessments: a design science approach. *European Journal of Information Systems*, Forthcoming,

Paquette, S., Jaeger, P. T., & Wilson, S. C. (2010). Identifying the security risks associated with governmental use of cloud computing. *Government Information Quarterly*, 27(3), 245-253.

PCI (2013). PCI SSC Data Security Standards Overview Archived at https://www.pcisecuritystandards.org/security_standards/index.php

Pearson, S. (2013). On the relationship between the different methods to address privacy issues in the cloud. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 8185 LNCS*, pp 414-433, Springer, Berlin.

Pearson, S., Mont, M.C., Chen, L., & Reed, A. (2011). End-to-end policy-based encryption and management of data in the cloud. In *3rd IEEE International Conference on Cloud Computing Technology and Science, CloudCom, 2011; Athens; Greece*, pp 764-771, London, Athens.

Ryan, M. (2010). Viewpoint: Cloud Computing Privacy Concerns on Our Doorstep. *Communications of the ACM,* 54(1), 36-38.

Ryan, M. D. (2013). Cloud computing security: The scientific challenge, and a survey of solutions. *The Journal of Systems and Software*, 86(9), 2263-2268.

Seddon, J. J. M., & Currie, W. L. (2013). Cloud computing and trans-border health data: Unpacking U.S.and EU healthcare regulation and compliance. *Health policy and technology,* 2(4), 229-241.

Swanson, E. B., & Ramiller, N. (2004). Innovating mindfully with information technology. *MIS Quarterly,* 28(4), 553-584.

The Economist (2010). Tanks in the cloud (29 December) Archived at http://www.economist.com/node/17797794

The Guardian (2013). Prism (7 June -) Archived at http://www.guardian.co.uk/world/prism

Venters, W., & Whitley, E. A. (2012). A Critical Review of Cloud Computing: Researching Desires and Realities. *Journal of Information Technology*, 27(3), 179-197.

Wang, R. (2011). Monday's Musings: Lessons Learned From Amazon's Cloud Outage (25 April) Archived at http://www.forbes.com/sites/ciocentral/2011/04/25/mondays-musings-lessons-learned-from-amazons-cloud-outage/

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly*, 26(2), xiii-xxiii.

Whitley, E. A., Gal, U., & Kjærgaard, A. (2014). Who do you think you are? A review of the complex interplay between information systems, identification and identity. *European Journal of Information Systems*, 23(1), Forthcoming.

Willcocks, L. P., Venters, W., & Whitley, E. A. (2011a). 2) Cloud and the Future of Business: From Costs to Innovation: Challenges *Accenture and the Outsourcing Unit*, Archived at http://outsourcingunit.org/publications/Cloudreport2_challenges.pdf

Willcocks, L. P., Venters, W., & Whitley, E. A. (2011b). 5) Cloud and the Future of Business: From Costs to Innovation: Management *Accenture and the Outsourcing Unit* Archived at http://outsourcingunit.org/publications/Cloudreport5_management.pdf

Willcocks, L. P., Venters, W., & Whitley, E. A. (2014). *Moving to the Cloud Corporation: How to face the challenges and harness the potential of cloud computing.* Palgrave, Basingstoke.

ACKNOWLEDGEMENTS

An earlier version of this paper appeared in Willcocks LP, Venters W and Whitley EA (2014) Moving to the Cloud Corporation: How to face the challenges and harness the potential of cloud computing. Palgrave, Basingstoke. The authors are grateful for the helpful feedback of the editor and reviewers and conversations with colleagues on the BSC Information Privacy Expert Panel (IPEP).