Thunder Clouds or Clear Blue Skies – Business Use of ‘Cloud’ Services

John Douglas Thomson

As private and public sector organizations seek to develop policies and to manage the remodelling and restyling of their e-services, the ‘cloud’ arouses much interest and attention. ‘Cloud’ computing suppliers provide not only a service to store data on behalf of customers but also provide applications and data analysis services. The paper’s purpose is to examine how business organizations can address the risks in using ‘cloud’ computing, offering new insights from the legal profession as an analogy. An inductive interpretivist narrative is used with the conclusion providing new insight and a distinctive contribution into how businesses can be guided by the legal profession in its use of ‘cloud’ computing technology, and the reality that information whether in electronic or physical form is susceptible to theft, loss or inadvertent disclosure.

Key words: ‘cloud’, computing, trust, transparency, legal, business, lawyers, jurisdiction, vendor.

Field of Research: Management (Contemporary issues in management, business ethics, e-commerce).

1. Introduction

‘Cloud’ computing is a term given to using someone else’s servers connected to the internet to store data, host applications or perform similar tasks where reliance is on those servers and the internet rather than on owned computers and related systems (Legal IT Lawyers, 2011). ‘Cloud’ computing is a form of remote electronic data storage on the internet, and promises to be the single biggest growth area in ICT (Thomson, 2011a). Data stored in the ‘cloud’ are maintained by vendors and stored on large servers that may be located anywhere in the world. E-government agencies are anticipating efficiency and effectiveness gains from the evolution of new business models and have the problem of attempting to adopt and adapt these new technologies to public sector e-business in order to achieve the benefits being realized by the private sector (Thomson, 2012, p40). There may also be problems associated with generational issues (Thomson, 2011b p554). Typically, the vendor purchases and maintains its hardware and software which business freely accesses on a rented basis and so outsources its ICT requirements. There are advantages using this protocol from a resourcing and cost perspective, but there are risks in the range of emerging ‘cloud’ alternatives being marketed from dedicated private communication solutions to multi-tenanted public solutions (Thomson, 2011c p249). Finding the balance between risk and advantage requires

John Douglas Thomson, GSBL, RMIT University, 405 Russell St, Melbourne. Email: doug.thomson@rmit.edu.au
consideration of ethical issues, the most significant of these being confidentiality and the control of private information (Thomson, 2011a). Entrusting data to other service providers via the 'cloud' places a degree of control with them (Legal IT Lawyers, 2011).

Many executives in major organizations are used to managing steady state processes and systems, with few ready to accept and cope with the problems and difficulties of massive technological innovations (Thomson, 2006 p285). Mine (2010) suggests that business benefits of 'cloud' computing include lower costs, selectively more information security than the risks associated with commonly used electronic technology, improved safeguards against avoidance of document loss, and provision of continuous upgrading of software at minimal or no cost. There is also a significant reduction in the costs of electronic data management, being easier to identify and budget for monthly or annual costs – there are often no installation fees as the vendor usually takes care of updates including security, and is responsible for data storage and retrieval (McCaulay, 2011). The software programs may mimic the business’s currently used software programs or may be newer or more up to date, be continuously updated, and have more features than the current business software (McCaulay, 2011). But there will always be concerns about a new technology’s security and reliability (McCaulay, 2011), and businesses need to know with whom they are doing business, what business and what financial exposure they have at any particular point in time (Thomson, 2010 p244). As Widmer (2009) notes, it is no longer possible to establish which data protection authority has jurisdiction or oversight for the implementation of data protection requirements in a particular context. Szekely, Szabo & Vissy (2011) state that as technology becomes increasingly globalized so too do its ethical implications. Górniak-Kocikowska (2007) argues that typically, societies develop their own ethical systems by which the members of that particular society are expected to live.

The paper’s purpose is to examine how business organizations address the risks in using ‘cloud’ computing, offering the legal profession as an analogy. The findings provide new insight and a distinctive contribution into how organizations can be guided by the legal profession in the use of ‘cloud’ computing technology, and the reality that information whether in electronic or physical form is susceptible to theft, loss or inadvertent disclosure.

The paper first introduces ‘cloud’ computing, then provides a literature review describing the uniqueness of the analogy for organizations to draw upon the legal profession’s responses to and understanding of ‘cloud’ computing. Such analogy has not been examined by any previous research. An inductive interpretative methodology draws from illustrative legal concepts which are sourced predominantly from 2010 to the present from the USA. This is because there has been less relevant empirical and legal research publication in cloud computing from other countries. The predominance of the USA in the early development and application of ‘cloud’ technology meant business and legal dealing with these issues commenced earlier than in other countries, and is more advanced.
2. The Legal Profession and the Cloud

For businesses, be they private, public or not for profit, guidance if not leadership in ‘cloud’ computing could be derived from the practices of the legal profession. Lawyers act for business and so have always carried an ethical duty to safeguard confidential client information. In the USA, Comment 17 of the American Bar Association’s (2010a) Model Rule 1.6 states that ‘the lawyer must take reasonable precaution to prevent the [client] information from coming into the hands of unintended recipients’ (American Bar Association, 2010). However, there is no basis in The State Bar of Virginia (USA) Rules of Professional Conduct (2009/10) for an unqualified prohibition of lawyers managing their office software applications and client data using ‘cloud’ computing. Business and lawyers may share such protected information with third parties as needed to perform necessary office management functions. That is, if the business or lawyer exercises reasonable care in the selection of a third party vendor and secures an agreement, the vendor will safeguard the confidentiality of the information shared (McCaulay, 2011). In the past, business and lawyers have outsourced copying and document production to third party vendors with confidentiality of client information usually protected by contractual arrangements between the law firm and the third party vendor (McCaulay, 2011). In advisory opinions, the US State Bar of Virginia Standing Committee on Legal Ethics and Professionalism (2009/10) emphasized that lawyers must act competently to protect the confidentiality of information relating to the representation of their clients, including protecting both open and closed client files. The American Bar Association (2010a) Formal Opinion 95-398 states that outside service providers would be considered to be non-lawyer assistants under Model Rule 5.3. This defines a lawyer’s obligation to ensure that the conduct of the non-lawyer persons or entities they employ, retain or become associated with is compatible with the professional obligations of the lawyer. This includes internet businesses such as Google or Yahoo that offer ‘cloud’ computing contracts on a take it or leave it basis (McCaulay, 2011). In this regard, The State Bar of Arizona Ethics Committee has stated that a lawyer or law firm ‘is obligated to take reasonable and competent steps to ensure that the client’s electronic information is not lost or destroyed’ (The State Bar of Arizona 2009 Opinion 05-04). In order to do this, a lawyer must be competent to evaluate the nature of the potential threat to client electronic files and to evaluate and deploy appropriate computer hardware and software to accomplish that end (The State Bar of Arizona, 2009; Feinberg & Grossman, 2010; American Bar Association, 2010b; McCaulay, 2011).

The State Bar of Massachusetts Association Committee on Professional Ethics (2009) issued an ethics opinion that ‘a law firm may provide a third party software vendor with access to confidential client information stored on the firm’s computer system for the purpose of allowing the vendor to support and maintain a computer software application utilized by the law firm’. However, the law firm must ‘make reasonable efforts to ensure’ that the conduct of the software vendor ‘is compatible with the professional obligations of the lawyers’, including the obligation to protect confidential client information. There is no requirement to guarantee that a breach of confidentiality cannot occur when
using an outside service provider (Feinberg and Grossman, 2010; McCaulay, 2011). Lawyers are required to act with reasonable care to protect information relating to the representation of a client (The Massachusetts Bar Association, 2009; McCaulay, 2011). The State Bar of Nevada Ethics Committee (2010) concluded that as long as a lawyer exercises care in the selection of the vendor, has reasonable expectation that the vendor will keep the data confidential and inaccessible by others, and instructs the vendor to preserve the confidentiality of the information, the American Bar Association (2010a,b) requirements are met (The State Bar of Nevada Formal Op.33, 2006). A recent Alabama ethics opinion takes a similar approach (The State Bar of Alabama, 2010). Forsheit (2010) states that while lawyers are often of the view that they do not need to concern themselves with security controls for protecting sensitive information because they are already subject to existing ethics rules and standards governing the protection of privileged information, at the same time they are storing client data, often unencrypted in the ‘cloud’ with a third party. Forsheit (2010) suggests that ‘cloud’ computing, e-discovery and data security is the business of lawyers from a legal ethics perspective and from a best practices data security point of view. This view also applies to businesses undertaking activities using ‘cloud’ computing services.

3. Compelled Disclosure and Safeguarding

In dealing with ‘cloud’ vendors, business will need to consider issues relating to access to data, contractual provisions for disclosure of confidential information including data to third parties (via subpoena or other compulsory disclosure), and the non-destruction of ‘cloud’ provider records and backup media. Also, the ‘cloud’ vendor should disclose any security breaches, release customer data only if required by law, and should provide affected customers with prior notice of any compelled disclosure (McCaulay, 2011). A robust security management system that is based on an internationally accepted security framework to protect customer data (eg ISO 27001 should be maintained, and provide data to customers in an industry standard downloadable format. There is a need also to determine vendor roles and responsibilities for privacy and security accountability. Section 1.6 of the American Bar Association’s Model Rules of Professional Conduct forbids a lawyer from revealing information relating to representation unless a client gives informed consent or the disclosure is impliedly authorized. Also, Section 1.15 of the Model Rules requires that a lawyer appropriately safeguard any property received by a client for safekeeping.

Businesses and lawyers should seek information from their data storage vendors regarding the identity of persons who have access to the system and data, and whether and under what circumstances the provider’s personnel or any third party business partners are subject to confidentiality obligations (The Clio Team, 2011; Kewalframani, 2011). Businesses and lawyers should have a clear understanding of their vendor’s security practices, especially in the case of a security breach, as well as its encryption protocols and storage procedures (The Clio Team, 2011; Kewalframani, 2011). Businesses and lawyers should ensure that any data they forward to a vendor for uploading to the ‘cloud’
remains the sole and exclusive property of the legal entity. Vendors should be asked to disclose whether they use servers outside the parent country which may be subject to different laws and regulations (The Clio Team, 2011; Kewalframani, 2011).

4. Reasonable Care

Forsheit (2010) advises that in the information security and privacy law communities, there is discussion about the problem of ‘reasonable care’, that is, businesses or lawyers confusing compliance with security. Forsheit (2010) points out that the American Bar Association Commission of Ethics 20/20 Working Group on the Implications of New Technologies recognises that there may be a gap between technology related security measures that are ethically required and security measures that are merely consistent with best practices. It might be ill advised for business to use a ‘cloud’ computing vendor that does not comply with industry standards re encryption, but it is not necessarily unethical if a business decides to do so. Thus many lawyers and businesses who already use ‘cloud’ computing may take the view that they need not employ security best practices because it is technically not unethical for them to opt against doing so.

Reasonable care may include consideration of ensuring the ‘cloud’ vendor has an enforceable obligation to preserve confidentiality and security, and that the vendor will notify the business or lawyer if served with process requiring the production of client information. Investigating the provider’s security measures, policies, recoverability methods and other procedures to determine if they are adequate, may be necessary as well as employing available technology to guard against reasonably foreseeable attempts to infiltrate the data, or investigating the vendor’s ability to purge and wipe copies of the data and to move the data to a different host if the business or lawyer become dissatisfied or otherwise wants to change vendors. Periodic checks to reconfirm that the vendors security measures remain effective as technology changes need to be undertaken (American Bar Association 2010a,b; Forsheit 2010).

5. Confidentiality, Cost and Burden

Confidentiality particularly relates to the identification of people - such as medical information, financial account information, or credit card numbers. This raises concerns that clients are trusting a business with personal information with an expectation that it will be protected in accordance with the laws and standards applicable to everyone else. The American Bar Association’s (2010a,b) interest in this extends to providing adequate protection for devices such as laptops or having methods for deleting data remotely in the event that a device is lost or stolen and encouraging the use of strong passwords. Purging data from devices before they are replaced (eg computers, smart phones, copiers with scanners) and installing appropriate safeguards against malware (ie virus protection, spyware protection) become essential, as does installing adequate firewalls to prevent unauthorised access to locally stored data. Frequent back-up of data and updating computer operating systems to ensure
they contain the latest security protections is required. Configuring software and network settings to minimize security risks and encrypting sensitive information become necessary. Identifying metadata from electronic documents before sending them and avoiding wifi hotspots in public spaces as a means of transmitting confidential information are mandatory (eg sending an email to a client) (Forsheit 2010). The American Bar Association (2010a,b) also expressed interest in whether lawyers need to procure cyber insurance or cyber liability insurance in addition to traditional professional liability coverage (Forsheit 2010). In brief, the American Bar Association (2010a,b) is of the view that lawyers ‘may use an online data storage system to store and back up client confidential information provided the lawyer takes reasonable care to ensure confidentiality will be maintained in a manner consistent with the lawyer's obligations’. In addition, the lawyer should stay abreast of technological advances to ensure that the storage system remains sufficiently advanced to protect the client’s information, and should monitor the changing law of privilege to ensure that storing the information online will not cause loss or waiver of any privilege (Forsheit 2010). Businesses should take note.

6. Information Security, Confidentiality and Competence

Consideration needs to be given to the situation where a business has information to suggest that the cloud vendor’s security measures are no longer adequate. If a lawyer learns of a breach of confidentiality by the vendor, the lawyer must investigate whether there has been a breach of confidentiality of its client’s information and must notify clients. It must discontinue the use of the service unless the lawyer receives assurances that the problems have been sufficiently remediated (American Bar Association 2010a,b; Forsheit 2010). While some online systems are password protected and data stored is encrypted, most ‘cloud’ solutions do not encrypt the data and rely on the user to do so. This means that businesses or lawyers using ‘cloud’ services must monitor not only changes in the technology but also changes in the law relating to technology (American Bar Association (2010a,b; Forsheit 2010). Many businesses or lawyers do not encrypt their data, have not investigated their ‘cloud’ vendor’s security measures, and do not have a contract provision requiring that the ‘cloud’ vendor notify them in the event of a data breach (Forsheit 2010). Businesses finding themselves in this situation may be fortunate if they have the ability to retrieve their information and transfer to a different provider with better security measures without incurring significant cost and burden.

The State Bar of California (2010) Standing Committee on Professional Responsibility and Conduct has concerns about whether a lawyer violates the duties of confidentiality and competence owed to a client if using technology to transmit or store confidential client information when the technology may be susceptible to unauthorized access by third parties. In effect, before using a particular technology a lawyer must take steps to evaluate the level of security when using that technology including whether reasonable precautions may be taken when using the technology to increase the level of security. The legal ramifications to a third party who intercepts, accesses or exceeds authorized
use of the electronic information needs to be known by the business client, and the degree of sensitivity of the information. The possible impact on the client of an inadvertent disclosure of privileged or confidential information or work product, together with the urgency of the situation and the client’s instructions and circumstance, such as access by other client’s devices and communications become of significance (Forsheit 2010).

7. Methodology: Inductive Interpretive Narrative

Narrative is an interpretive approach in the social sciences involving storytelling methodology, where the story becomes an object of study, focusing on how individuals or groups make sense of events and actions in their lives (Mitchell & Eguado, 2003). They suggest theoretical underpinnings to narrative approaches and how narrative conveys tacit knowledge, how it can enable sense making, and how it constructs identity. Interpretivism is a school of thought in contemporary jurisprudence and the philosophy of law. Unlike deductive arguments, inductive reasoning allows for the possibility that the conclusion is false, even if all the premises are true (Vickers, 2010; Sandberg, 2005; Conroy, 2003). Instead of being valid or invalid, inductive arguments are either strong or weak, which describes how probable it is that the conclusion is true (Herms, 1984). The inductive methodology chosen for this research is but one way of interpreting ‘cloud’ problems. Induction suggests that nothing can be known with certainty except that which is actually observed (Vickers, 2010; Conroy, 2003). Critics of this approach claim that it is essentially descriptive and does not really explain anything as it fails to uncover the causes of the generalized observations. But ‘what has changed is the interpretation of ideas and problems … and the methodological pluralism approaches available to resolving them’ (Hughes, 2007 piii). Thus, an inductive interpretivist narrative is used

8. Business Outsourcing

The American Bar Association (2010a,b) acknowledges that ‘cloud’ computing is a form of outsourcing, and is concerned about the obligations of lawyers when outsourcing work to other lawyers and non lawyers, in particular in relation to ‘cloud’ computing requiring amendments to the American Bar Association’s Model Rule of Professional Conduct (2010a). The American Bar Association (2010a,b) acknowledges that due diligence and contract negotiation processes should be undertaken and, specifically, which terms and conditions are essential for lawyers to have included. These cover the ownership and physical location of stored data, the vendor’s back-up policies and the accessibility of stored data by the provider’s employees or sub-contractors. The vendor’s compliance with particular state and federal laws governing data privacy including notifications regarding security breaches is required as is the format of the stored data and whether it is compatible with software available through other providers. The the type of data encryption and the policies regarding retrieval of data upon termination of services must be known (Forsheit 2010). Under American Bar Association (2010a,b) Model Rule 5.3, a lawyer who employs, retains or associates with a non-lawyer must make reasonable
efforts to ensure that the person’s or business’s conduct is ‘compatible with the professional obligations of the lawyer’. Lawyers or businesses who outsource must ensure the tasks are delegated to individuals who are competent to perform them, and must oversee the execution of the outsource is performed satisfactorily and appropriately.

9. Business Ethics Committees

For many business, intellectual property protection and client confidentiality is very important. But documents and information are never really secure online or offline. Mine (2010) is of the view that the risks posed by ‘cloud’ based platforms are little different from the ordinary risks to information confidentiality that are encountered in the current online or offline worlds. Since ethics committees are not technology experts and do not regulate the confidentiality of every communication or document storage, Mine (2010) suggests that special standards should not be required for ‘cloud’ based computing. Imposing minimum levels of security or requiring passwords for all ‘cloud’ based users would impede communication, and ethics committees have traditionally applied a reasonable expectation of privacy in determining the ethics of a particular technology. Technology changes so fast that ethics committees are unlikely to be able to keep up, and business executives may be more interested and effective than ethics committees in judging whether a particular technology offers a reasonable expectation of privacy and security (Mine, 2010). Further, rather than focus on the expectation of privacy, business ethics committees should advise executives to assess risks in determining the appropriate level of security to employ to meet ethics obligations.

10. Industry Codes

The recommendations of The State Bar of Massachusetts Committee on Professional Ethics highlighted the importance of agreed standards to ensure consistency of ‘cloud’ computing services which in turn are expected to assist in the establishment of trust. The use of voluntary industry codes is advanced as a beneficial and cost effective alternative to legal statute. Sethi (2006) suggests that industries often prefer to develop voluntary codes as a means of establishing technical and quality standards for products, contracts, services and other arrangements that create economies of scale so reducing transaction costs (Williamson, 1993). Sethi and Emelianova (2006) suggest voluntary codes represent a series of undertakings that their contributors promise to honour and to address real or perceived societal concerns. They describe voluntary codes as a type of ‘private law’ or a ‘promise voluntarily made’ whereby a business makes a public commitment to certain standards of conduct. They argue that industry groups prefer this approach because it allows them to project and magnify their efforts at minimum cost with minimal changes to their production system.

An industry code provides businesses with a mechanism by which they can develop economically efficient solutions to those concerns held by members of a society, taking into account industry needs. Sethi (2003) and Kapstein (2001)
suggest that industry codes have the effect of engendering public trust through 'reputation effect'. From the public's perspective, voluntary codes obviate the need for costly further governmental regulation with the possibility of onerous regulatory conditions. O'Rourke (2003) suggests they provide the avenue by which moderate elements among the affected groups may seek reasonable solutions to the issues involved. However Sethi and Emelianova (2006) also state that the success of a voluntary code is based on the ability to create and maintain high levels of public credibility. A code is a form of voluntary 'private law'. It does not reduce the duties of a business or a lawyer, rather, it potentially increases the need for transparent measurements and reporting systems (preferably by a third party) so that its sceptics, critics and the public-at-large believe in the industry’s or business’s responses or claims.

11. Business Disaster Recovery

Business and lawyers using 'cloud' computing have a right to know where the servers will be located and data processed and stored, what the disaster recovery plan and back up is, where the support service is based and who will have access to sensitive data. There is also the need to have the right in advance to approve transfer of data to another country, to know the different levels of access, who is in charge of the specific project for the business and if there monitoring and third party auditing of policies and procedures (McCaulay, 2011). While the US Federal Trade Commission and the European Union have laws protecting the privacy of information that may affect users of ‘cloud’ computing in their jurisdictions, (McCaulay, 2011), the ‘cloud’ computing service provider may move the data for its own reasons to another server in another country without notifying the client. This could result in unintended consequences for the business or lawyer.

‘Cloud’ computing vendors should be required to explain their information handling practices and disclose the performance, location and reliability of their services. Further, a ‘cloud’ vendor should claim no ownership rights to customer data and should use customer data only as its customers instruct or to fulfill contractual or legal obligations (McCaulay, 2011). For example, data may be subject to discovery in pending or anticipated litigation. This may require a business or lawyer to make reasonably diligent efforts to comply with a legally proper discovery request by an opposing party (McCaulay, 2011).

12. Conclusion

As with any emerging technology, reputable businesses must confront ethical issues that arise when using a new technology. Such ethical challenges revolve around issues of trust which are difficult to establish and maintain on the internet. In order to address these problems both voluntary industry codes and legal frameworks may provide a means to establish clear performance and quality standards. However, the very nature of ‘cloud’ computing being offered in one location when it is physically located in another, often undisclosed to the user, creates problems of compliance and jurisdiction. Businesses should be conscious that there may be some information that is just too sensitive, too
critical or too valuable to be stored in the ‘cloud’, and that when it comes to technology, what is ‘reasonable’ is constantly changing (Kewalframani, 2011).

It is necessary for ethical businesses to conduct due diligence before making any decision to dispatch data to the ‘cloud’, to ensure the online computer data storage vendor used has an enforceable obligation to preserve confidentiality and security, and that the vendor will promptly respond if required to produce client documents, files or records relating to a transaction or proceeding. ‘Cloud’ computing may have much to offer business but it is not without its risks. In assessing the costs and benefits of outsourcing to the ‘cloud’, business may want to think about the possibility that certain information may be a better candidate for ‘cloud’ computing than others. In this sense, ‘cloud’ computing creates interesting ethical tensions between cost and security, trust and transparency. The key finding is that the legal profession’s use of ‘cloud’ services provides a good standard for consideration by businesses when outsourcing to the ‘cloud’.

References


Sandberg, J., 2005, How Do We Justify Knowledge Produced Within Interpretive Approaches? Organizational Research Methods, Vol. 8 No. 1, January 41-68, Sage Publications;


Sethi, SP., and Emelianova, O., 2006, A failed strategy of using voluntary codes of conduct by the global mining industry, Corporate Governance, Vol. 6 Iss: 3, pp.226 – 238;


The Clio Team, 2011. Legal Cloud Computing Association Published Responses to ABA, North Carolina State Bar, NC, USA, Jul;


The State Bar of Massachusetts Association, 2012, Opinion 12-03 of the Committee on Professional Ethics, Massachusetts, USA:

The State Bar of Nevada, 2010, Nevada Ethics in Government Manual, Nevada Commission on Ethics, July; Carson City, Nevada USA;


