Private Clouds with No Silver Lining: Legal Risk in Private Cloud Services

Rebecca IGLESIAS, Rob NICHOLLS & Anisha TRAVIS
Webb Henderson, Sydney, Australia

Abstract: This paper provides an overview of the legal risks that arise from the use of private clouds arising from lawful interception, data protection obligations and legal professional privilege. The paper uses an Australian perspective to provide examples, but concludes that there are significant legal risks in all jurisdictions.

Key words: cloud computing, private cloud, lawful interception, data protection, professional privilege.

Cloud computing, sometimes referred to as utility computing, is a broadly used term that has spawned a myriad of competing industry definitions. There is an extensive literature on the subject including a substantial body of recent work (AL-QIRIM, 2011; ARMBRUST *et al*., 2010; BUYYA *et al*., 2009; JOINT *et al*., 2009; NABIL, 2010; PAQUETTE *et al*., 2010; RITTINGHOUSE & RANSOME, 2009; THOMPSON & van der WALT, 2010).

For the purposes of this paper cloud computing is a model for on demand network access to computing resources such as servers, software and data storage with minimal service provider interference. Various deployment models for cloud services have been developed, the most common being public clouds and private clouds. Public clouds involve computing resources being provided to end-users over the Internet via web services from service providers to anyone who wishes to use the cloud. Private clouds are delivered over public or (virtual) private networks usually for the exclusive benefit of a single organisation, which has specified its level of control over the data storage and technical quality of the cloud. The growth of cloud computing, particularly the ability to store data in multiple jurisdictions simultaneously, has raised concerns over the dangers of this new computing model. There has been much debate over the difficulties that may be encountered in terms of data protection, privacy and interception laws with public clouds, however, private clouds appear to have escaped much of the

academic and industry discourse concerning questions of jurisdiction and compliance. At first glance, private clouds appear to eliminate many of the difficulties concerning data protection and compliance regimes facing public clouds. This is because they have highly limited access to the content and data within the cloud. Private clouds do not get publicity that attracts hackers to large public clouds, especially those which are free to all users such as those offered by Google. However, the analysis in this paper demonstrates that private clouds are not immune to the legal issues surrounding utility computing. The paper focuses on three issues facing private clouds under existing legislation:

- telecommunications interception by law enforcement agencies (LEAs);
- data protection and jurisdiction issues; and
- commercial obligations in the form of legal professional privilege and the use of private clouds to store client communications.

The paper uses Australia as an example of a jurisdictional approach, but also indicates the relationship between approaches in Australia and elsewhere. Indeed, the cross-jurisdictional nature of cloud computing compounds the risks in deployment of cloud solutions.

The use of the term "private" in relation to cloud solutions is misleading. A private cloud is not immune to interception, search and seizure requests by LEAs. Private clouds are no safer than any other form of telecommunications to data access requests. In some jurisdictions even if data is stored offshore, the operators of private clouds, as the data controllers may have an obligation to provide LEAs with access to that data. the operator makes data available to anyone other than to a properly authorized LEA.

The European Union, among other jurisdictions, has strict privacy laws relating to the storage and transfer of data to the extent that data can only be transferred outside of the EU if the recipient jurisdiction has acceptable data security laws or standard form contracts are in place. Private clouds, which involve limited data access, seem like a perfect solution to meet the standard requirements for transferring data. However, private clouds do not create an automatic safe haven for the purposes of EU data transfer laws.

Legal professional privilege exists over communications and documents intended to be confidential between a legal practitioner and a client. This exists to protect the client and there is a strict duty on lawyers to store their client's information and communications safely. Private clouds are a viable means of storing this data. However, practitioners must use caution. An

externally managed private cloud may open practitioners up to liability for negligence. Encryption may be necessary. If lawyers' private clouds do not have adequate security leading to compromise of data security, privilege could be lost.

■ Clouds

There has been much industry complaint over the use of the term "cloud computing" as a marketing buzzword. The recent increase in its use has led to the development of an array of different definitions in both industry and academic circles. This paper uses the definition provided by the National Institute of Standards and Technology (NIST):

Table 1 - Service models in cloud computing

Service	*Model*
Software as a service (SaaS)	SaaS involves a central hosting on the internet of software and applications which circumvents the need for the end-user to install the software on a hard drive. The most common example of this is web-based email services. Individuals can choose to sign up to an email service created and operated by a third party, accessible anywhere in the world, (e.g. Gmail). The program uses a web browser and no dedicated software is installed on an end-user's device.
Infrastructure as a service (IaaS)	IaaS provides the end-user with the benefit of normal computing hardware such as server and storage space and access to a network as a service. The user gains the capabilities that computing hardware provides as if they had access to that hardware, but, as a practical matter, the user is given a proportion of the capabilities of the pooled resources of a powerful data centre.
Platform as a service (PaaS)	PaaS provides the underlying set of programming functions, configuration settings and protocols to run the applications and utilise the cloud. The end-user is provided a preconfigured operating system or platform to access the infrastructure and software.

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud computing can utilise three service models (National Institute of Technology Standards, 2009) as set out in table 1.

Software as a service (SaaS) has existed for a relatively long time, leading some commentators to claim that cloud computing is nothing new but merely a marketing gimmick (ARMBRUST *et al*., 2009). It is only in recent years that infrastructure and platforms have been unbundled and delivered as a utility in the same way as software to form a holistic package known as cloud computing (ARMBRUST *et al*., 2009). There are five main characteristics of cloud computing identified by NIST (2009) which are useful not only in conveying the advantages of the service but also in differentiating clouds from more mainstream computing models. These characteristics are set out in table 2.

Table 2 - Characteristics of cloud computing

Characteristic	*Description*
On demand self service	Computing capabilities such as bandwidth and storage can be acquired by the user as they are needed without any human interaction with the service provider.
Broad network access	Cloud computing is based on networks which are accessible from any standard platform.
Resource pooling	Cloud service providers pool resources to serve multiple consumers and to give the illusion of unlimited bandwidth and processing power. Resources are assigned according to demand.
Rapid elasticity	Capabilities can be scaled outwards and inwards depending on demand levels at any time.
Measured service	Cloud systems use a metering capability not only to re-provision services in line with consumer demand, but also to monitor the use of those resources to provide a transparent account of usage and associated costs.

There are four current deployment models for cloud services: public clouds, private clouds, hybrid clouds and community clouds. This paper examines the first two deployment models, public and private but the analysis focuses on private cloud.

In a public cloud, access to the cloud and its resources are provided to multiple customers simultaneously over the Internet via Web services from a third party provider on a pay-as-you-go system rather than upfront payments (ARMBRUST *et al*., 2009). Current examples of public clouds include Microsoft Azure, Amazon Web Services and Google Apps.

Private clouds, on the other hand, use public and virtual private networks with data centres that have outside firewalls for the exclusive use of a single organisation. The customer specifies control over the data, security and quality of the cloud (ARMBRUST *et al*., 2009). Only organisation members with clearance can access the cloud and access is subject to whatever safety procedure the organisation thinks necessary. They involve private

data centres and servers never made available to the public. Private clouds are often managed externally by a third party provider although they can be created and maintained by a company's IT department.

The discourse in academic and industry circles concerning cloud systems has acknowledged the various difficulties cloud computing faces in terms of ensuring privacy and adequate data protection and in complying with local laws and regulatory frameworks. Discussion tends to acknowledge private clouds as a method of overcoming these difficulties by shifting the data to a private network designed for and controlled by a single organisation. However, this is an oversimplification of the benefits of private cloud systems, which are arguably faced with the same legal challenges as their public counterparts. There appears to be a gap in the academic and industry literature concerning the potential legal limitations and liabilities of private clouds in circumventing privacy and data storage concerns as well as how existing telecommunications interception and access laws apply to private cloud systems. This paper seeks to partially address that gap by focusing on three prominent areas of legal risk for cloud computing systems:

- telecommunications interception by LEAs;
- data protection and jurisdiction issues; and
- commercial obligations in the form of legal professional privilege and the use of private clouds to store client communications.

As the analysis shows, private clouds are not a blanket solution to the legal risks facing advances in technology. Private clouds generate all of the same concerns as their public counterparts, albeit on a somewhat lesser scale. Indeed, in the context of responding to telecommunication access requests and warrants from LEAs, company directors of organisations with private cloud computing systems will encounter potential criminal charges if they incorrectly divulge private data. There are legal risks to both using and commercially operating private cloud systems. The term "private" when applied to cloud computing does not reduce the complex array of legal consequences facing the sector.

■ Private clouds and telecommunications interception and access regimes

This paper uses the Australian lawful interception regime as the basis for an analysis of the types of risks that arise form the lawful interception of, and

access to, communications. The Australian *Telecommunications (Interception and Access) Act 1979* (Cth) (the TIA) recognises two forms of communications for the purposes of interception prohibition:

- communications passing over a telecommunications network (e.g. live or near real- time communications); and
- stored communications.

A stored communication refers to any form of speech, text, images or data that is not passing over a telecommunications system and is held on equipment operated by and in possession of a carrier and which cannot be accessed by a person not party to the communication without the assistance of the carrier.

The TIA makes it an offence, punishable by imprisonment, to intercept or access either class of communication or to permit another person to intercept or access such communications. However, there is an exception to the general prohibition for the purposes of law enforcement agencies with an interception warrant or a stored communications warrant. Stored communication warrants can be accessed by all enforcement agencies (including public revenue agencies) while interception warrants can only be accessed by law enforcement agencies. This includes B-Party warrants, which target the communications of innocent third parties who communicate with a person suspected of a serious offence (SELVADURAI & ISLAM, 2010, p. 383).

Australia's internal security agency, ASIO, receives special treatment under the TIA and can access both stored communications and intercept the communications of a person named on a warrant issued by the Attorney General if the communications are being used by a person reasonably suspected of engaging in activities prejudicial to security (NICHOLLS & ROWLAND, 2007, p. 88). ASIO's powers of access and interception apply across all forms of telecommunications systems, and telecommunications content contained within a private cloud can be the subject of ASIO's powers of interception.

The TIA also imposes obligations on carriers and carriage service providers to provide assistance to relevant law enforcement agencies as is reasonably necessary for certain purposes. These purposes include protecting national security and enforcing criminal law. Carriage service providers must establish interception capabilities, including the ability to provide "telecommunications data" (in reality, metadata such as the date, length and recipient of communications) on a prospective or near real time

basis, on a request, not a warrant, from an LEA, which has been certified at a senior level (NICHOLLS & ROWLAND, 2008, p. 346). "Telecommunications data" was left undefined in the Act, which means that it is possible for data from all forms of telecommunication devices and systems, including private clouds, to realistically be included in an LEA request (NICHOLLS & ROWLAND, 2008, p. 349). This effectively means that the scope of the term "telecommunications data" will be defined by LEA demands, which appears to be a concerning trend towards self-regulation.

A telecommunications service provider or carrier provides access to private clouds. This is the case regardless of whether the cloud is created and maintained by an in-house IT department or purchased and maintained by a cloud service provider. Consequently, even though the cloud is "private", requests for reasonable assistance including access to telecommunications data within the cloud will generally be lawful. LEAs may request that the service provider provides access to telecommunications data such as the metadata associated with access to the cloud. So long as those requests are reasonable, the carrier is under a legal obligation to comply irrespective of whether the cloud is private or not. In this context, a private cloud does not have the level of data security that some commentators and vendors claim. Private clouds are just as susceptible to interception and access requests as any other form of telecommunications system.

Taken as a whole, the system of reasonable assistance requests is particularly worrying in the context of its application to private clouds. Carriers must comply with such requests unless they are willing to demonstrate that such a request is unreasonable. LEA assistance requests are by no means an unusual occurrence given that there were more than 250,000 of these requests in 2009 (NICHOLLS, 2009, p. 70). These requests usually relate to telecommunications data under the Act and this covers metadata associated with almost all forms of communications. Communications metadata for corporate entities is often highly sensitive. Given the lack of any legal precedents governing the area of private clouds that might increase data security, users and operators of cloud services should take into account the consequences of assistance requests by LEAs. Further, the contents of private cloud system may be the subject of access and interception warrants from LEAs.

Another potential liability arises in terms of private clouds and data access and interception in the form of the potential criminal liability that may come from incorrectly disclosing information. There is a balance that carriers

have between providing the required assistance to LEAs and their obligation not to disclose communications. The willingness of service providers to assist LEAs has been documented (NICHOLLS & ROWLAND, 2007) and this potentially reduces the data security, which might be assumed of a private cloud.

Many LEAs have unrealistic ideas concerning how much information can be retrieved from deleted communications and this often creates a great deal of complexity for operators to perform searches for materials in question. Search warrants can also be very broadly directed, with simple keywords such as "building" or "bomb" or in the case of financial enforcement agencies, "tax office" or "scheme" (NICHOLLS, 2007, p. 92). The tendency towards broad scope keyword searches may mean that private cloud providers are forced to yield highly sensitive corporate information that has been communicated via email. While private cloud computing systems certainly have their benefits, they are not immune from the operation of normal law enforcement mechanisms. That is, "private" does not mean "inviolate".

■ International data security standard and private clouds

Data protection and security laws differ in various jurisdictions; however, with the rise of cloud computing systems, the problem of reconciling the various legal regimes around the world has become increasingly problematic. Perhaps the most stringent data protection regime is that of the European Union as articulated in Directive 95/46/EC, commonly known as the Data Protection Directive (the Directive). The Directive covers the storage and processing of the personal data of EU citizens in the context of the right to privacy. The definition of personal data in the Directive is very broad and covers any information relating to an identifiable natural person, known as the data subject, including credit card numbers, bank details, place of residence, etc. It also extends to any method of processing that data including saving, retrieving or transmitting it. The Directive and the domestic legislation of individual European states based on the Directive ban the transmission of personal data to countries outside of the EU unless those countries have "adequate" data protection laws. At the time of writing, the data protection regime in the USA has not been declared "adequate" for the purposes of the EU Directive. This means that the personal data of EU citizens cannot be sent to the USA. This is problematic for multinational

corporations, which often have several offices in diverse geographic locations. Private clouds are no more an exception to this prohibition on third country transfer than public clouds are. If firm X with offices in both London and New York had clients based in the UK and intended to have the New York office work on matters for London-based clients, putting the data on a private cloud which relies on a data centre based in the USA would breach the *Data Protection Act 1998* (UK) which implements the Directive.

In order to utilise a private cloud without breaching EU data protection laws, the organisation which holds the personal data of EU citizens (known as the data controller) will need to guarantee that the third-country recipient will comply with the EU data protection regime. In early 2010, the European Commission released a series of standard contractual clauses that can be used to transfer data to third countries without acceptable data protection laws. The data controller (who for the purposes of the contract becomes the data exporter) must warrant that the data importer in the third country jurisdiction will comply with EU protection laws during and after the transfer. The data importer must similarly warrant and guarantee that it has in place appropriate storage and security measures and will apply with appropriate EU data laws and standards. In the context of private clouds, where a single organisation with regional or international offices imports the data, each office must be a separate legal entity in order to enter into the contract validly, and similarly, this contract must be repeated in every jurisdiction with access to the data, leading to an array of almost identical contracts within an organisation.

If the data importer for some reason cannot comply with EU laws and standards, or there has been some form of unauthorised access to the data by a third party, or a request for access to data has been made by a law enforcement agency, it must inform the exporter. The standard form contract also includes clauses for the purposes of liability if the data subject has suffered damage due to breaches on the part of the importer. Importantly, the governing law of the contract must be that of an EU state; in some jurisdictions, including the USA, the third party rights of a data subject to damages for breach of contract and access to the contractual terms would be almost impossible to enforce due to issues with privity of contract.

However, this is not all that is needed to synchronise private clouds with European data protection laws. If the private cloud is run by an external service provider (known as a "sub-processor"), then the contract with the service provider must include clauses concerning the provider's compliance with EU laws and create a notification regime to ensure prompt notice if

there are any breaches of the provider's data security software. Under the European Commission's standard form contract, the data importer must warrant that they have received guarantees from the sub-processor that the security systems and protocols in place to safely store the data meet EU standards. In order for the importer to fulfil this contractual obligation to the exporter, they must ensure that their initial contract with their service provider contains clauses to this effect, or they must negotiate with their service provider to vary the terms of the existing contract in order to meet these obligations.

In effect, data transfers involving private clouds and personal data originating in any European Union jurisdiction will necessitate a complex series of contracts which will have to include a notification system for data loss, intrusion or attempted intrusion that is foreign to most IT entities outside of Europe. If the data exporter chooses to use the model standard clauses, the fact that the choice of law must be that of the EU country from which the data is exported will come as an unpleasant shock for multinational organisations. These are accustomed to using choice of law as a means of minimising liability by specifying the law of a state with under-developed privacy controls. If the data exporter attempts to circumvent this clause, they may run foul of national supervisory bodies that oversee data processing in the EU member states.

On 25 January 2012, the European Commission unveiled a draft legislative package to overhaul the previous data directive and create a unified pan European data policy which would create a single standard of end-user protections. The new regime applies explicitly to all corporate organisations functioning in the European Union, regardless of whether they were incorporated in the EU or not. In terms of its effect on cloud computing, data transfers via clouds may become easier under the new regime as transfers will be deemed safe if the corporate entity to which the data is transferred adopts a strict set of corporate rules regarding data processing. The rules must be legally binding and they must clearly set out the rights of the data subject in a legally enforceable manner so that the data subject may sue upon a breach of those rules. If adopted, this package is likely to reduce the need for an onerous contractual agreement that was the hallmark of the previous regime in its interaction with cloud computing.

■ Legal professional privilege in the cloud

Legal professional privilege protects a client's documents and communications to their lawyer from disclosure and is one of the foundations of the Western legal tradition, usually existing at both common law and in statute. The privilege exists for the benefit of the client rather than the practitioner and ensures that clients are free to make full disclosure when seeking legal advice without fear of the information being used against them later. For example, to attract the privilege at common law in Australia, the communications or documentation must be or have been intended to be confidential and the legal advisor must have been acting in their professional capacity in receiving the communication or preparing or using the documents. Almost identical requirements for a statutory version of legal professional privilege called "client legal privilege" are set out in legislation.

In most common law countries, legal privilege is waived in situations where the holder of the privilege communicates the contents of privileged documents to third parties. As privilege exists to protect communications of a confidential nature between practitioners and clients, communications as to the contents of the documents in question is held to be inconsistent with the supposedly confidential nature of the documents and thus the existence of privilege.

In Australia, the position on waiving privilege was given further clarity in Commissioner of Taxation *v* Rio Tinto Limited (2006) where it was held that even indirect or accidental communications could jeopardise the existence of privilege. In the context of private clouds, it could be that poor security procedures or even detailed file names could destroy the privilege if too many people within an organisation can freely access legal documentation. For example, if a practitioner's advice was saved by a client in a folder within the cloud that was accessible to several hundred people within an organisation who are not involved in the legal aspects of that organisation, privilege may have been waived. Furthermore the accessible nature of confidential legal advice in the cloud could lead to situations where the advice is summarised and provided to outside parties or internal committees and board members, particularly if those with access to the documents were not briefed by practitioners on how to maintain the privileged nature of the documents. In this context, summaries of legal advice given to committees or board meetings within an organisation in Australia are likely to waive legal privilege.

The U.S. position regarding privilege is slightly different, as the case of Upjohn v United States held that legal privilege will still attach to documents even if those documents are viewable by some low ranking employees who do not have management duties. The U.S. position is also further complicated by a myriad of different state laws concerning who can waive the privilege; in most cases inadvertent slips by attorneys may be enough to waive privilege while other states provide more stringent protections on privilege. However, despite the difference, there is a common thread running through the common law position: practitioners must fulfil their duties to advise clients by ensuring that the client is aware of the potential for privilege to be lost in a private cloud setting.

Legal professional privilege is not inviolate and can be waived by the client, but not by the lawyer. If a client is reckless about storing or otherwise keeping safe and private a certain document or communication, a court may reach a finding that the conduct was in a manner inconsistent with the supposed privileged nature of the document or communication and hold that the privilege has been waived. This is on the basis that privilege only attaches to confidential communications and that carelessness implies that the nature of the document or communication was not confidential.

This leads to issues for private clouds. If a private cloud lacks adequate security and data is compromised, in subsequent litigation it may be found that the material has lost its confidential character and therefore its privileged status. It does not matter whether an outsider or a rogue employee perpetrated the data loss or there is an overall systems breach and certain documents are either copied or stolen. Lawyers have a duty to advise their clients in relation to their legal liabilities including those associated with client storage of data. To meet this duty, practitioners must notify their clients on the potential waiver of privilege that reckless storage of documents on poorly protected private clouds may lead to. This may lead to lawyers recommending that their clients demand (by contract) adequate and effective data security systems including warranties on encryption.

For lawyers, a duty of confidentiality exists concerning their clients' communications that extends to safely and securely storing such information. Negligently storing or disclosing a client's information can lead to disciplinary action from professional registration groups as well as malpractice suits. Ironically, many lawyers in commercial practice have failed to realise the potential liability attached to private cloud storage while advising clients on large-scale corporate cloud projects. Practitioners need to consider the potential liability and the wishes of their clients when deciding

whether to switch from their current IT systems to private cloud technology. To avoid any possible negligence suits practitioners may need to advise their clients as to where their private cloud's data centre is located (i.e. the physical real world storage space for the data in the cloud). Such advice would be impossible in a public cloud ecosystem.

The shift to cloud computing, like any shift in technology, has led to an intense debate over how to apply existing legal ethics to a new form of technology. The propensity of public clouds to be hacked, or for accidents in data partitioning and storage to occur, as well as difficulties regarding the ability of the service providers to access sensitive information and difficulties with data search warrants, are well known disadvantages which have rendered the legal profession wary of shifting to cloud computing. In order to safeguard sensitive client information, and avoid malpractice suits, legal professionals have generally only considered private clouds. However, shifting client data onto private clouds may not provide adequate protection for sensitive information. Further safeguards may be necessary to avoid negligence suits, particularly given the relative ease with which firewalls and encryption programs can be utilised.

Law societies in the United States have been proactive in providing guidance as to how practitioners can meet their legal duties while utilising private clouds and it is reasonable to assume that the U.S. jurisprudence in this area will influence the common law position as it develops. US ethics committees have indicated that highly sensitive client material including emails should be encrypted before being put on even a private cloud (State Bar of California, Standing Committee on Professional Responsibility and Conduct 2010). However, the situation in the US is different given that some state jurisdictions hold that inadvertent and accidental disclosure of privileged information by attorneys is a waiver of the privilege.

Most other jurisdictions are far more lenient when there are inadvertent slips or disclosures by practitioners of privileged material. There has been a trend in other professions with strict ethics concerning client information to encrypt sensitive data before storing it in a cloud. Healthcare providers in the US have begun encrypting patient data before storing it on a private cloud system or otherwise enhancing the security of their private clouds with firewalls or packet filters. While some authors maintain certain data should never be placed on clouds as a means of safeguarding privileged content, this is arguably going too far. Reasonable care must be taken to safeguard privileged documents and communications. This includes encrypting data and ensuring security measures and not simply relying on the private nature

of the cloud as an adequate safeguard. However, this does not remove the duty of legal practitioners to inform their clients as to the potential loss of privilege that may attach to the client storing legal advice or related communications on a private cloud that lacks requisite security measures.

There is also a further aspect of private cloud systems that is problematic to legal practitioners - who maintains the private cloud. Private clouds can be run in one of either two ways:

- an internal IT department can create and maintain the cloud if their expertise and capacity allows; or
- a private cloud system can be purchased from a third party service provider who maintains the cloud.

If a law firm with multiple offices in different locations chooses to operate a private cloud using an in-house IT team, care must be taken in deciding which jurisdiction is chosen. Some jurisdictions such as the US extend legal professional privilege to those hired to perform ancillary legal roles, such as secretaries and IT professionals, while others do not (FREEMAN, 1999, p. 48). Externally managed private clouds also have their own fair share of potential difficulties. It is important to ensure that there are reasonable safeguards in place to prevent employees of the service provider from accessing confidential information when performing maintenance. Confidentiality clauses may need to be inserted into contracts for private cloud systems in order to bolster the security of the cloud.

■ Conclusion

Cloud computing is another phase in the evolution of IT services and like all advances in technology, presents challenges in terms of its interactions with existing laws and regulatory schemes. Like their public counterparts, private clouds engender complex interactions with the laws of various jurisdictions. Adopting industry best practice will ensure that many risks are minimised but simply relying on the private nature of the computing system to ensure security is a gross overestimation of the capabilities of private clouds. Private clouds are not immune from existing telecommunication access and interception laws and will open the possibility for private organisations to be forced to liaise with LEAs and potentially be served with search and seizure warrants. Cloud owners and service providers will need to tread carefully when faced with LEA requests and warrants. In terms of

data protection and transfer, private clouds do not circumvent the growing international difficulties with EU data protection laws facing multinational corporations when information is accessed, copied or transferred to another jurisdiction. In order to export or store data concerning European citizens outside of the European Union where the receiving jurisdiction does not have acceptable data protection, a complex series of contracts will have to be negotiated between the organisation in Europe and its offshore storage or access facility. These must ensure that the offshore entity warrants to follow the relevant domestic version of the EU Data Protection Directive. If the offshore entity controlling the cloud has bought their cloud from a service provider who also provides a maintenance service for that cloud, then the entity will have to contract with the cloud provider to ensure that EU data protection laws are complied with. Finally, in terms of legal professional privilege and the use of private clouds, there remains a prevailing view that simply retaining sensitive client data on a private cloud is enough to maintain privilege. Should a breach of security occur in a private cloud system, it is likely that a court will look at the presence and robustness of internal security systems including the encryption of data within the cloud in order to impute whether or not the practitioner was treating the data in a manner inconsistent with its confidential nature. The overreliance of practitioners on the private nature of the cloud may lead to documents being considered that they were never intended to be confidential and thus losing their privileged character.

In short, there is no silver lining to private clouds in terms of potential legal risks.

Bibliography

AL-QIRIM, N. (2011): "A Roadmap for success in the clouds", *International Conference on Innovations in Information Technology (IIT)*, 2011.

ARMBRUST, Michael, Armando FOX, Rean GRIFFITH, Anthony D. JOSEPH, Randy KATZ, Andy KONWINSKI, Gunho LEE, David PATTERSON, Ariel RABKIN, Ion STOICA & Matei ZAHARIA (2010): "A view of cloud computing", Commun. ACM 53(4):50-58.

European Commission (2010): Commission Decision: on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, *Official Journal of the European Union*, L 39/5.

FREEMAN, E. (1999): Attorney - Client Privilege and Electronic Data Transmission, *Information Systems Security*, 7(4).

JOINT, Andrew & Edwin BAKER (2001): "Knowing the past to understand the present - issues in the contracting for cloud based services", 27, *Computer Law and Security Review*.

JOINT, Andrew, Edwin BAKER & Edward ECCLES (2009): "Hey, you, get off of that cloud?" *Computer Law & Security Review*, 25(3):270-274.

MASON, S. & E. GEORGE (2011): "Digital evidence and 'cloud' computing", 27, *Computer Law and Security Review*.

MELL, P. & T. GRANCE (2009): The NIST Definition of Cloud Computing.

NABIL, Sultan (2010): "Cloud computing for education: A new dawn?" *International Journal of Information Management*, 30(2):109-116.

National Institute of Standards and Technology (2009): *Information Technology Laboratory*, Version 15.

NICHOLLS, R. & M. ROWLAND:

- (2007): "Message in a bottle: Stored communications interception as practised in Australia", presented at: *From Dataveillance to Uberveillance and the Realpolitik of the Transparent Society: The Second Workshop on the Social Implications of National Security*, K. Michael & M. G. Michael, Canberra, University of Wollongong.
- (2008): "Lost in Transcription: the Australian regime for interception of, and access to, communications content and metadata", *Record of the Communications Policy & Research Forum*.
- (2008): "Regulating the use of telecommunications location data by Australian law enforcement agencies", 32(6), *Criminal Law Journal*.

NICHOLLS, R. (2009): "For What it's Worth: Cost Benefit Analysis of the use of Interception and Access in Australia", presented at: *The Fourth Workshop on the Social Implications of National Security*, Canberra, Australian National University.

NORISWADI, I. (2011) "Cursing the Cloud (or) Controlling the Cloud?", 27, *Computer Law and Security Review*.

PAQUETTE, Scott, Paul T. JAEGER & Susan C. WILSON (2010): "Identifying the security risks associated with governmental use of cloud computing", *Government Information Quarterly*, 27(3):245-253.

RITTINGHOUSE, J.W. & J.F. RANSOME (2009): *Cloud computing: implementation, management, and security*, CRC Press.

SELVADURAI, N. & R. ISLAM (2010): The expanding ambit of telecommunications interception and access laws: The need to safeguard privacy interests. 15 Media and Arts Law Review.

State Bar of California (2010): Standing Committee on Professional Responsibility and Conduct Formal Opinion No. 2010- 179.

THOMPSON, Willem J.J. & Jakobus S. van der WALT (2010): "Business intelligence in the cloud", *SA Journal of Information Management* 12(1), Art. #445.