Cloud computing issues for legal practices

When legal data and client information are entrusted to the cloud, law practices need to be aware of issues surrounding its accessibility, integrity, security and confidentiality.

By CORALIE KENNY *and* TAHLIA GORDON

Coralie Kenny is a councillor of the Law Society of New South Wales; Tahlia Gordon is research and projects manager with the Office of the Legal Services Commissioner.

The term 'cloud computing' generally refers to anything that involves delivering hosted services over the internet.[1] These services are offered from data centres all over the world, which collectively are referred to as the 'cloud'. Any user with an internet connection can access the cloud and the services it provides. Since these services are often connected, users can share information between multiple systems and with other users. Cloud computing is simply a way to describe how individuals and organisations can take some or all of their existing IT infrastructure and operations and hand it over to someone else to build or manage.

Over the last few years, we have seen a considerable growth in scale and sophistication of cloud computing services. Web-based email services like Gmail and Hotmail deliver a cloud computing service in which users can access their email 'in the cloud' from any computer with a browser and internet connection, regardless of what kind of hardware is on that particular computer.

Cloud computing is a way of delivering higher levels of security, availability, performance and flexibility for business IT infrastructure, with minimal or no capital expenditure.

To help legal practitioners ensure they meet their ethical and professional obligations when using new technologies such as cloud computing, the Law Society of NSW, in conjunction with the Office of the Legal Services Commissioner (OLSC), is developing a series of guidelines which will be based on the findings of a major research project by the OLSC. By way of introduction and to contextualise the guidelines, a series of short papers is being published in *LSJ* to inform the profession of the relevance of these topics to legal services and to identify the professional conduct issues to be dealt with in the guidelines. The first article, on social media, appeared in *LSJ* April 2012; the second article in *LSJ* May 2012 covered outsourcing. This is the third and final in the series.

Cloud computing and legal practice

Depending on how it is applied by a legal practice, cloud computing offers legal practices a great many opportunities to alter their service delivery. It can increase the mobility of the workforce by removing the need to be physically located at the office, and allow services to be accessed and paid for as they are used, avoiding the greater overhead of maintaining dedicated equipment, software and support resources.

A range of technology exists to facilitate virtual practice today. Email, file-sharing applications and audio/video conferencing applications (such as Skype, GotoMeeting or GlobalMeet) for example, are free general technological tools that can be used to communicate with clients and manage files online. There also exists a variety of specific legal online management systems that offer document management and storage platforms, secure document and information exchange services, secure email networks, digital dictation services and billing/timekeeping services. A number of online management systems provide trust management, general practice accounting, time recording and simple payroll services for users.

For legal practices wishing to have a purely virtual practice, specific cloud computing software can be installed that allow legal practices to store client data, financial records, legal documents, and other information on the internet, rather than house data in servers physically located on their premises. Several providers allow clients to discuss matters online, download and upload documents for review, diarise, handle billing, invoicing, and payments online, complete online forms, and handle other business transactions in a secure digital environment. These providers do so by offering users a secure, password-protected portal enabling clients to interact with a firm online, view documents drafted online, pay legal bills via an online payment system, look at documents related to their matter 24/7 via web-based access, and be notified of important events about their matter by logging into the website.

Advocates of cloud computing cite a number of advantages compared with traditional practice. They include lower costs due to reduced overhead, less hassle related to maintaining and upgrading the case management system and greater flexibility, since the web-based system can be accessed anywhere, at any time. Online document storage also benefits clients. Clients no longer have to call the office to request a copy of a document in their file. Instead, the client can simply access the entire file at their convenience using the online platform. Another benefit is that clients do not need to take time off from work to meet with their legal practitioner for simple document review and revision. Instead, legal practitioners who use web-based document management technology can offer clients the option to collaborate in real time.

The issues

By far the greatest concern for solicitors who access cloud- computing services for their legal practices is the potential for breach of confidentiality or security that can take place with regard to any client information that may be held in a cloud computing environment operated by a third party. The locating of client information in the cloud and out of the direct physical control of the legal practitioner leaves it potentially vulnerable to unauthorised access or inadvertent disclosure.

The sources of potential security threats are twofold. First, there are external threats including third parties, such as hackers. Even data held by Google, one of the largest cloud-computing providers, for example, is not immune from hackers.[2] Second, there are internal threats, for example, employees of the cloud computing provider accessing the data without authorisation. In the context of this latter threat, cloud computing providers can organise their systems such that employees have minimal access to client data. This can be done at both a technical level (password access control and restricting access to physical equipment) and a legal level (contractual requirements of confidentiality). However, such actions can never guarantee absolute security.

"Legal practices should, at least, consider informing their clients that they are using a cloud computing service provider."

In addition to the security risks presented by storing data in the cloud, there are also reliability issues associated with cloud storage. While the data might not be accessible to unauthorised parties, the data must be accessible to the lawyer whenever it is required. By placing data on the cloud and making its availability the responsibility of a third party, the legal practitioner risks losing control over when they can access its data.

The cloud computing provider may, for example, be temporarily unable to provide the data to the lawyer. This may be due to some technical reason beyond the control of the provider, such as an extended blackout, industrial action or natural disaster or suspension of service due to late payment of service fees. The cloud computing provider may become insolvent or otherwise permanently unable to continue offering its services. Lawyers using a cloud computing service may find themselves temporarily unable to connect to the internet for some reason beyond their control. Data that becomes temporarily inaccessible can clearly have profound consequences for a lawyer or law firm if work needs to be done urgently for the client.

Conflicts of interest present another concern. A new potential client who contacts a virtual law firm through its online system might, for example, present a concurrent conflict if the virtual law firm is already acting for the opposing side in the dispute, or a successive conflict if agreeing to represent the new client will involve the virtual law firm possibly using confidential information of a former client to the disadvantage of that former client in the new dispute. Some virtual law firm software includes conflict checking mechanisms that can automatically compare parties' details to identify conflicts.

For example, some SaaS (software as a service) products include a conflict of interest check built into the application and have been set up to search for the names of any party associated with cases selected by the legal practitioner running the check.

However, there is always room for error.

Effective supervision is another concern when cloud computing services are used. Supervising the technical operations of many interconnected computer systems, entities, and personnel that may span the globe may be challenging. In virtual law firms, for example, the "lack of physical proximity and sporadic work arrangements may create firms with more attenuated relationships among lawyers who service the firm's clients, making supervision of work, communication among lawyers and the assurance of competent client representation more difficult".[3] Therefore, it is crucial for managers and supervising legal practitioners in virtual law firms to ensure appropriate procedures and systems are established so that professional and ethical obligations are met. One approach suggests that ad hoc teams with a "horizontal pattern of information flow and supervision" could be used as a method of restructuring law practices from the traditional vertical channel approach.[4] Such models attest to the changing nature of the lawyer-client relationship.

Cloud computing also raises concerns about data protection. Under most standard terms of service, a cloud service provider claims the right to move, store, and process a customer's data. The customer is given no right to receive reports on the exact whereabouts or jurisdictional location of its data, the number of copies made of such data, or the locations where such copies may be stored. Unlike a fixed server in an office or at a data centre in Australia, data in the cloud could potentially be located anywhere in the world and even in multiple data centres in multiple copies worldwide. There are at least four possible applicable jurisdictions for the information at any given moment: the location of the service provider's headquarters, the location of the servers, the location of the legal practice and the location of the communications equipment transmitting the information between the provider and the user (if such location can be readily determined).

Data may thus be subject to concurrent telecommunications and privacy laws and the powers of government in a number of jurisdictions. The US Patriot Act, for example, declares the US Government's right to access anything it wants from any cloud infrastructure over which it can claim jurisdiction. Similarly, Singapore has more than 160 disparate, sector-specific laws regulating the use and disclosure of data in Singapore, and failure to comply with these laws may prove costly. The government can issues fines and/or revoke operating licenses, which in turn risks damaging the cloud computing company and the legal practice's reputation.

What to consider

Solicitors using cloud computing technology should consider a number of issues when entering into arrangements with service providers including:

- ☐ where the cloud is hosted;
- ☐ who is hosting the cloud;
- ☐ who has access to the cloud facility, the servers and the data;
- ☐ what mechanisms are in place to ensure that only authorised personnel will be able to access your data;
- ☐ how frequently back-ups are performed;
- ☐ whether data is backed up to more than one server;
- ☐ where the respective servers are located;
- ☐ whether data, and any back-up copies always stay within Australia;
- ☐ security of the data centers where the servers are housed;
- ☐ whether they will be notified if there is a data breach; and
- ☐ how costs for remedying the breach are allocated.

Legal practices should, at least, consider informing their clients that they are using a cloud computing service provider. ☐

ENDNOTES

1. For a more formal definition of cloud computing see the frequently cited definition by the National Institute of Standards and Technology, Special Publication 800-145, available at *http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf*.
2. T. Claburn, "Twitter hack tars Google's cloud" 16 July 2009 InformationWeek *www.informationweek.com/news/internet/google/218500810*.
3. L. Levin (2001), "Preliminary reflections on the professional development of solo and small law firm practitioners", 70 *Fordham Law Review* 847.
4. J. Kashi (1994), "Technology and economic are changing how you practice law", 20 *Law Practice Management* 44. ☐