Cloud services

By Kylie Day and Caroline Dobraszczyk

Cloud computing services are a relatively new development, which some members of the Bar are finding helpful in the management of their practices. What do we mean by 'cloud'? Basically, we mean someone else's computer servers. At its most simplistic, cloud services involve being able to store and/or share selected electronic files on remote servers owned or operated by others, so that you can access those files via the internet from multiple electronic devices, and share them with others if you wish. Without going into the technical detail here, different cloud services do have different technical and processing attributes.[1] They exist in many variations, including data storage sites, video sites, tax preparation sites, personal health record websites, photography websites, social networking websites and many more.[2] There are numerous providers of cloud computing services, such as Dropbox, ZipCloud, SugarSync, Microsoft SkyDrive, and Google Drive. Information is readily available about them on the internet, including their Terms of Service and policies. There are also websites which review and compare various cloud computing services and provide tips and buying guides (see eg http://www.thetop10bestonlinebackup.com/), although these may not be focussed on aspects of the services which are of most concern to barristers (such as security issues).

Benefits

There seem to be two main benefits for a barrister of using a cloud computing service. First, it enables one to access one's electronic documents from different computers, devices and locations, avoiding the need to email documents from one computer to another computer or take hard copies with you (if you want to work on a document in chambers and also at home, for example). If a document is stored in a cloud, you should be able to access it from any computer or device with an internet connection. Secondly, using a cloud computing service can make collaborating on documents easier. If you store a document (say, submissions) in a cloud, you should be able to grant access to others to work on it and then store the revised version. In other words, the use of a cloud computing service should enable documents to be accessed, worked upon, and stored in a manner which is more like that with which many barristers will be familiar from time spent working as solicitors within firms.

Risks

However, storing and sharing documents in a 'cloud' raises legitimate questions and concerns as to the effect that this may have on the ownership, security, confidentiality and privilege of documents. A cloud provider's terms of service, policies, and location may significantly affect these matters. It is impossible

to deal with these matters comprehensively in an article of this kind. However, one of the best things that you can do, if you are contemplating use of a cloud service, is to read and compare the Terms of Service of some of the providers. These generally deal with matters of ownership, security and privacy, among other things that you will be interested in. The way in which the provider manages the risks to your documents, or creates additional risks, will vary, and some Terms of Service will be more attractive to you than others. Of course, no method of electronic storage is 100% secure. While the risks of cloud storage (as opposed to other methods of electronic storage) should not be overstated, paying particular attention to your choice of service provider and its Terms of Service will be one of the most important ways in which you can deal with the risks that storage poses for the security, confidentiality and privilege of your documents.

Ownership

The first issue is that of ownership, that is, who owns the documents stored with the 'internet company' which is providing you with the cloud storage service? The short answer is that it depends on the Terms of Service that you agree to. The standard Terms of Service for cloud storage services vary as to what effect, if any, the use of the service has on the ownership of and rights in the documents. The following are some of the current standard terms from Dropbox, Microsoft SkyDrive and Google Drive:[3]

From Dropbox -

> Your stuff and Your Privacy: By using our Services you provide us with information, files, and folders that you submit to Dropbox (together, 'your stuff'). You retain full ownership to your stuff. We don't claim any ownership to any of it. These Terms do not grant us any rights to your stuff or intellectual property except for the limited rights that are needed to run the Services …

From Microsoft's SkyDrive -

> 3. Content. … Except for material that we license to you that may be incorporated into your own content (such as clip art), we don't claim ownership of the content you provide on the services. Your content remains your content, and you are responsible for it. We don't control, verify, pay for or endorse or otherwise assume any responsibility for the content that you and others make available on the services.

From Google Drive:

> Your Content in our Services. Some of our Services allow you to submit content. You retain ownership of any intellectual property rights that you hold in that content. In short, what belongs to you stays yours.
>
> When you upload or otherwise submit content to our Services, you give Google (and those we work with) a worldwide license to use, host, store, reproduce, modify, create derivative works (such as those resulting from translations, adaptations or other changes we make so that your content works better with our Services), communicate, publish, publicly perform, publicly display and distribute such content. The rights you grant in this license are for the limited purpose of operating, promoting, and improving our Services, and to develop new ones. This license continues even if you stop using our Services …

So, although you may retain the ownership of documents and files that you put in a cloud, you are likely to be granting to the provider of the cloud service the right to use that material:

- at the very least, to the extent that that is necessary to run the service (eg, by reproducing your files where they are to be stored); and
- in some instances, for the purpose of the cloud service storage provider promoting and improving their services and developing new ones.

Clearly, the control that you have over your documents will be affected when you place them in a cloud. And particularly where the Terms of Service are of the kind imposed by Google Drive, there is uncertainty as to what use may ultimately be made of your material.

As one observer has noted (at a time when concerns were being expressed about Google Drive's introduction of the Terms of Service set out above):[4]

> If you look at the Terms for all sorts of online services you'll find similar language explaining that you're granting non-exclusive, royalty free rights to distribute your photos, words, or other data.
>
> But that doesn't mean the whole outcry is much ado about nothing. It's good to be reminded every now and again that even if a cloud service isn't directly asserting ownership of the files you upload-you *are* giving up a certain level of control over those files when you decide to share them. That's true whether you are posting on a public site such as

> Flickr or a more private service such as Dropbox where your files can only be seen by the people you share them with.
>
> If you want to make absolutely certain that nobody will ever see your content, turn it over to the feds when subpoenaed, or otherwise breach your privacy, the best thing to do is probably to horde all of your data on a local hard drive. But you lose the benefits of a cloud-based service such as the ability to easily share files, publish them for the world to see, or protect your important data which might be lost if your local hard drive happens to fail.

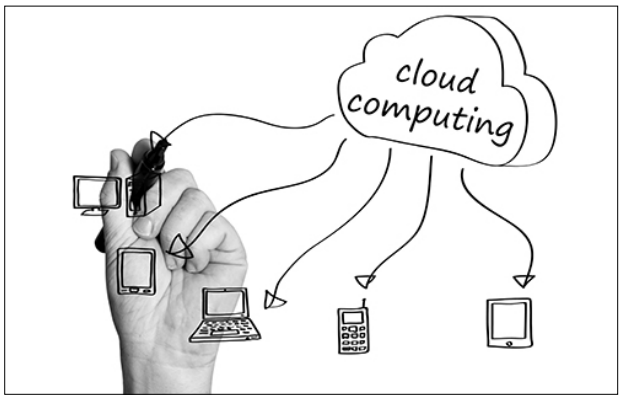
That last paragraph brings us squarely to the important issues of security and confidentiality, and as to whether a middle path exists whereby barristers can use cloud services, with all their attendant benefits, while taking sufficient precautions to manage the risks to the security, confidentiality and privilege of their documents.

Security, confidentiality and privilege

As the authors of a recent report on cloud storage have noted, it is easy to exaggerate the difference a cloud makes. Although it is a new development, in many ways it is just an extension of existing practices and technologies. Most documents are now digital and networked, and they are already easily copied and moved between locations or jurisdictions.[5]

Traditional hosting or server hire contracts involve the use of someone else's storage or computers. However, it would normally be clear who you are dealing with, and where your rented resources are. Those arrangements are unlikely to be established on a casual or informal basis. That is true at least for barristers' own computer servers – but as soon as documents are emailed to a solicitor, for example, it is unlikely that a barrister will have knowledge or control of those matters. Similarly, with cloud storage the ultimate location(s) of your documents (and the jurisdiction(s) to which they are subject) may be unclear, possibly even unidentifiable. Also with cloud storage, it is much easier to set up (and change) those arrangements, and documents may be stored in multiple locations and multiple jurisdictions.[6]

Cloud services are often based in data centres in places like the USA, central Europe or Singapore, which offer cost and other benefits. Differences



between the regulatory frameworks that exist where the data is hosted, where the hosting companies are based, and where the data subjects or users are based, can create complex legal and compliance issues. Some of this risk cannot be fully offset by contracts or technology alone.[7] The legal and technical support for adequate online security, confidentiality, privacy and data protection varies widely between countries. International agreements such as the *Convention on Cybercrime* from the Council of Europe (CETS 185, in force in Australia from March 2013) arose to address this in some areas. However, many countries are not a party to relevant agreements and some of them have quite underdeveloped legal coverage of online issues generally. In addition, those countries which are parties to a Convention may have varying implementations of its model laws. For example, the USA and Italy have exposed their citizens to less of the effects of the Convention than Australia has. In other words, rights and obligations may not be reciprocal. Clearly, the practical implementation of security and confidentiality, and the degree of protection of Australian – owned documents and data from third party access, will vary according to these and other local factors.

In 2009 the World Privacy Forum reported on issues surrounding privacy and confidentiality in the cloud computing environment in its 'White Paper: Privacy in the Clouds'. A summary of its findings included the following, which succinctly capture the risks associated with the use of cloud storage services:[8]

- A user's privacy and confidentiality risks vary significantly with the terms of service and privacy policy established by the cloud provider. The risks may be magnified when the cloud

provider has reserved the right to change its terms and policies at will. The secondary use of a cloud computing user's information by the cloud provider may violate laws under which the information was collected or are otherwise applicable to the original user.

- There are obligations that may prevent or limit the disclosure of some records to third parties, including the providers of cloud services. For example, health record privacy laws may require a formal agreement before any sharing of records is lawful. Other privacy laws may flatly prohibit personal information sharing by some corporate or institutional users. Professional obligations of confidentiality, such as those imposed on lawyers, may not allow the sharing of client information, and the sharing of information with a cloud service provider may undermine legally recognised privileges (see further below).
- When a person stores information with a third party (including a cloud provider), the information may have fewer or weaker privacy protections than when the information remains only in the possession of the person. Government agencies and private litigants may be able to obtain information from a third party more easily than from the original owner or creator of the document.
- Any information stored in the cloud eventually ends up on a physical machine owned by a particular company or person located in a specific country. That stored information may be subject to the laws of the country where the physical machine is located. For example, personal information that ends up maintained by a cloud provider in a European Union Member State could be subject permanently to European Union privacy laws.
- A cloud provider may, without notice to a user, move the user's information from jurisdiction to jurisdiction, from provider to provider, or from machine to machine. The legal location of material placed in the cloud could be one or more places of business of the cloud provider, the location of the computer(s) on which the information is stored, the location of a communication that transmits the information from user to provider and vice versa, and possibly other locations.
- The laws of some jurisdictions may oblige a cloud provider to examine the records of users for evidence of criminal activity and other matters.
- The law generally trails technology, and the application of old law to new developments can be unpredictable.

It is conceivable that the provision of material to a cloud provider (and other third parties) may affect the existence and maintenance of any applicable privilege in respect of it. The law of privilege can be complicated; it varies depending on the privilege at issue, depending on whether statute or common law applies, and depending on the jurisdiction. However, at least in some situations, the communication of privileged material to a third party can affect whether or not any privilege arises and, if so, whether or not it has been 'waived'.

It is conceivable that the provision of material to a cloud provider (and other third parties) may affect the existence and maintenance of any applicable privilege in respect of it.

Whether the storage of a privileged communication or document with a cloud provider actually affects privilege is likely to depend on the terms under which the service is offered. For example, as the World Privacy Forum has suggested,[9] if the provider merely stores material, and disclaims the right or ability to look at it, the argument that any privilege continues to inhere in the material ought be stronger. However, if the cloud provider has the right to read, disclose, transfer and use material entrusted to it (eg, as per the Terms of Service for Google Drive), privilege is likely to be more difficult to maintain. These matters would bear further and more detailed consideration (including analysis of some of the standard Terms of Service of the most common cloud service providers), and we propose to deal with this in a separate article.

In addition, barristers need to bear in mind their obligation of confidentiality, for example under

Rules 108 to 111 of the NSW Barristers' Rules. None of the exceptions to the obligation of confidentiality specifically deal with disclosure to a cloud or other service provider, although disclosure with the consent of the person to whom the barrister has an obligation of confidentiality would appear to be permissible.

US laws impacting on security and confidentiality

Given that many cloud services are offered by companies based in the USA, you may be interested to consider some of the laws which apply to them and may impact on the security or confidentiality of documents that they store. At the outset, it is important to bear in mind these matters of common sense:[10]

> As a practical threshold item, … the US government is usually interested only in matters that concern US interests, for example, payment of US taxes, crime in violation of US laws and threats to US national security. Much of the information held in cloud stores under US jurisdiction on behalf of foreign data owners may be of little interest to them for this reason. But … it is apparent that US authorities will not apply particular self-restraint in scenarios involving foreign jurisdictions and US interests.

These are important considerations when weighing up the benefits of using cloud services versus the likelihood of your documents being seen by third parties without your consent.

It will come as no surprise that there are numerous ways in which a US company (or indeed any company in the world), which provides cloud services, may have to disclose either subscriber details or even the content of the documents it hold. A summary of some of these is as follows (and is drawn from the more detailed review in Chapter 5 of the recent report by the UNSW Faculty of Law's Centre for Cyberspace Law and Policy):[11]

- The US government may make informal information requests. Many US companies are willing to comply with such requests, to cooperate with the US government on issues of shared interests (eg fraud prevention on e-commerce sites). Some companies are also obliged to comply with certain information requests. For example, telecommunication service providers have to provide access for law enforcement purposes under the *Communications Assistance for Law Enforcement Act* of 1994.
- A summons, subpoena, warrant or compliance with disclosure rules by the company in the course of litigation could very well mean that not only your details (ie as a subscriber to the service) but also the contents of documents may need to be disclosed.
- There are specific powers under US legislation which may mean that your documents are disclosed (eg the *USA Patriot Act* of 2001). This legislation was enacted after the terrorist acts of 11 September 2001, to expand the US government's powers to obtain data for investigations in connection with international terrorism and foreign intelligence. This legislation had the effect of lowering the previous thresholds for the activation of powers in existing legislation by amending the *Foreign Intelligence Surveillance Act* of 1978 ('FISA') and other legislation governing a process known as 'National Security Letters'.
- Some specific powers of law enforcement agencies under the FISA, which may constitute potential risks for those hosting data in the US, include:
  - The power of the FBI to compel the production of any 'tangible thing' for the purposes of an investigation to obtain foreign intelligence or protect against terrorism and other intelligence activities;
  - The power to conduct secret physical searches of personal property, without a warrant, for investigations in which foreign intelligence gathering is a significant purpose. The person whose property is searched need not be directly involved, and the search may be conducted without a warrant, provided that the Attorney General certifies that there is no substantial likelihood that the property of a US person is involved;
  - There is power to obtain a search warrant in all criminal investigations without providing notice to the subject for up to 30 days or longer if a Court permits;

- there is power to conduct roving wiretaps on communications lines;
- the Department of Justice has power to grant approval for law enforcement agencies to engage in electronic surveillance without a court order for up to one year for the purposes of obtaining foreign intelligence (this power again is based on there being no substantial likelihood that a US person is a party to the communications).

- As noted above, the US Patriot Act also amended other legislation governing a process known as National Security Letters. These are a type of federal administrative subpoena. Essentially, the FBI may, without court approval, use a National Security Letter to compel individuals and businesses to provide a variety of records including customer information from internet service providers. A National Security Letter may be issued to any person who the issuer believes may hold information relevant to a terrorist or other intelligence investigation. This process has been the subject of much legal and political controversy.[12]
- The US has also entered into numerous mutual legal assistance treaties including the Council of Europe's Convention on Cybercrime. The cooperation under these arrangements can mean the sharing of electronic information between law enforcement authorities in the relevant countries.[13]

The primary limit on the United States Government's power to obtain information is the Fourth Amendment of the US Constitution, which prohibits 'unreasonable searches and seizure'. Under the Fourth Amendment, the government must obtain a warrant supported by probable cause that a crime has been committed, that describes 'the place to be searched and the persons or things to be seized', and provides simultaneous notice of the search to the person. Whether a search and seizure is 'reasonable' depends on whether the person has an objective 'reasonable expectation of privacy', in the item subject to the search. However, the protection provided by the Fourth Amendment is not absolute and one exception is known as the 'third party exception'. That is, a person does not have a reasonable expectation of privacy if he or she discloses the information to a third party.[14] The Centre for Cyberspace Law and Policy has noted that:[15]

> In the context of electronically stored data, the US government has routinely relied on this Third Party Exception to dispense with the warrant requirement. Federal courts take the view that a person does not have a reasonable expectation of privacy in the subscriber information that he or she provides to an internet service provider…..
>
> At least one court took a different approach and held that whether a person has a reasonable expectation of privacy in subscriber information provided to an ISP depends in part on the ISP's terms of service.

There is also federal legislation in the US directed to protecting the privacy of electronic communications (the *Electronic Communications Privacy Act 1986*, which includes the *Wiretap Act* and the Stored Communications Act). However, it has been widely criticised by consumer groups, privacy advocates and companies as ineffective in protecting privacy in light of technological changes; they have called for its reform.[16] Critics contend that inconsistent standards may be applied to the same information, pursuant to the Fourth Amendment and the Electronic Communications Privacy Act, depending on the form in which the information is held at any particular point in time, and there has been inconsistency in the decisions of courts on these matters, which creates uncertainty for companies who host content, as to how the law applies to material on their systems. In its recent report, the Centre for Cyberspace Law and Policy stated that:[17]

> For example, the Eleventh Circuit held that individuals do not have a reasonable expectation of privacy in read e-mail messages stored with an ISP because they 'shared' them with the service provider. In contrast, the Ninth Circuit held that an electronic communications service provider who turns over opened and store text messages without a warrant or a viable exception is liable under the SCA for making an access that was not permitted 'as a matter of law'. To confuse matters more, a panel of the Sixth Circuit held that users have a reasonable expectation of privacy in e-mails, only to have its decision reversed by the Sixth Circuit sitting *en banc* on grounds that the plaintiffs did not have standing to sue, but without addressing the constitutionality of the SCA provisions. (footnotes omitted)

As a result of this ambiguity in the law, critics have proposed a variety of changes to the *Electronic Communications Privacy Act* of 1986.[18]

Some suggestions for users of cloud services

Some barristers appear to be treading a middle path, between the extremes of hoarding everything on a local hard drive, and putting everything in a cloud. One colleague says that he uses cloud storage like a 'knapsack'. He is selective about what he puts in it, and the time for which he leaves it there; password protection and encryption can assist in maintaining the security and confidentiality of documents, although they are not failsafe.

However, as the World Privacy Forum has sensibly observed, users of cloud services need to be vigilant and may need to avoid using cloud services for some classes of documents or information, while being able to select a service that meets their privacy and confidentiality needs for other categories of documents and information. The Forum has recommended that each user of a cloud provider pay more – and indeed, close – attention to the consequences of using a cloud provider and, especially, to the provider's Terms of Service.[19]

... users of cloud services need to be vigilant and may need to avoid using cloud services for some classes of documents or information,

One way of alleviating some of the concerns outlined above may be to use a cloud service that commits to hosting material on servers within national boundaries. However, even if material is hosted domestically, it is conceivable that some service providing access to the data could be hosted in a foreign jurisdiction, or under the control of another jurisdiction.[20] Even where you try to require a cloud provider to keep data within the geographic borders of your country, it cannot be assumed that you will only be subject to your own country's laws because, in certain circumstances, cloud providers may be legally obliged to communicate information, including confidential personal information, to authorities in other countries.[21] Similarly, domestic hosting does not deal with issues that may arise (particularly in the context of privilege), as a result of the provision of your material to the third party cloud service provider. The issue of privilege needs to be carefully considered by barristers in the context of use of cloud service, about which we will write more shortly.

Endnotes

1. *Data Sovereignty and the Cloud* by David Vaile, Kevin Kalinich, Patrick Fair and Adrian Lawrence for the Cyberspace Law and Policy Centre, UNSW Faculty of Law, Version 1.0, July 2013, pp.7 - 10.
2. *Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing,* a report prepared by Robert Gellman for the World Privacy Forum, 23 February 2009, at p 4.
3. All of these quoted terms were available online at the time of writing: see https://www.dropbox.com/privacy#terms, http://windows.microsoft.com/en-AU/windows-live/microsoft-services-agreement, and http://www.google.com/intl/en/policies/terms/
4. Brad Linder, 'Dropbox, Cloud Storage and Who Owns Your Files?', article published on 3 July 2011 on Liliputing at http://liliputing.com/2011/07/dropbox-cloud-storage-and-who-owns-your-files.html
5. *Data Sovereignty and the Cloud*, at pp.3-4.
6. Ibid., at pp. 3, 12.
7. Ibid., at p.16.
8. *Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing,* at pp.6–8.
9. *Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing,* at p.10.
10. Ibid., p.32.
11. *Data Sovereignty and the Cloud*, Chapter 5, pp.31 – 48.
12. Ibid., pp.39–40.
13. Ibid., p.46.
14. Ibid., at p.34.
15. Ibid., at p.35.
16. Ibid., at pp.41 – 42.
17. Ibid., at p.42.
18. Ibid., at p.42.
19. *Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing,* at pp 7–8.
20. *Data Sovereignty and the Cloud*, p.15.
21. Ibid., p.17.