Using the cloud in the legal profession

by  **Martin Curilla**, LL.M., DLA PIPER

Cloud computing has become one of the most profitable, well-established segments of global information technology services. In EU alone, the cumulative economic impact of cloud computing has been predicted to stand at €940 billion and 3.8 million jobs for the period of 2015-2020[1].

At its simplest, cloud computing is a way of delivering computing resources as a utility service via a network on a location-independent basis, typically through the Internet, with the possibility to scale the service up and down depending on user requirements. The services provided by cloud computing can range from providing raw processing power and storage to delivery of full software applications. Accordingly, a wide range of devices such as mobile phones, tablets or notebooks may be used to obtain access to vast computational resources. Law firms as well as solo practitioners around the world have quickly adopted cloud services in their everyday work precisely because of the unique features that cloud computing can deliver.[2] Nevertheless, concerns may arise when taking into consideration the importance of confidentiality and security of information that law firms usually handle. There are significant differences between the security and service features of cloud products developed specifically for the legal community and those developed for the general public. The aim of this article is to briefly address the most common considerations that a law firm or a lawyer should take when deciding whether to use the cloud in the legal profession.

Review the Service Level Agreement ("SLA") in detail

The SLA should always be carefully reviewed in order to ensure that client data can be adequately protected and maintained in the cloud. At minimum, the following issues should be examined:

- Who owns the data? Although it is unusual for cloud providers to state that they own the stored data, the SLA should clearly state that attorney/law firm is the owner of the stored data;
- Who can access the data? The SLA should guarantee the access is kept to minimum and specify which employees will be authorized to access the stored information;
- Is the company adequately preserving data's confidentiality and integrity? The SLA should specify that data is encrypted not only when stored in the cloud but also during the data transmission;
- How does the company notify users if the data is subpoenaed? As cloud providers are private companies, they are obliged to comply with court orders to search the data stored on their servers. The attorney/law firm should nevertheless make sure that the SLA specifies the obligation to immediately notify the user of any legal attempts to access the data. SLA should also specify what steps will be taken if such event occurs and whether the cloud provider will challenge the attempt at court.
- What will happen to stored data in case the company goes bankrupt or is acquired by another entity? Although this issue is not typically included in standard SLAs, it should be raised before committing to the service.

Data security

In the legal profession, the confidence of the client is absolutely crucial. Accordingly, the client data needs to be secured in the best possible way against an unwanted intrusion. The cloud provider should be able to explain its firewalls and other security measures[3] that prevent such intrusion to a reasonable extent. Moreover, if the attorney/law firm grants access to client information to any third party, otherwise privileged information may lose its privilege and could be admitted as evidence before the court. It may be worth considering one of the cloud services that guarantee no access to the data, such as the increasingly popular SpiderOak cloud service with its zero-knowledge privacy policy[4]. Especially for clients with sensitive data, this option is gaining in popularity.

The location of stored data

As the confidentiality and accessibility of data is governed by the laws of the jurisdiction where the server holding the data is located[5], the attorney/law firm should assess whether the data privacy and data security legislation of the relevant jurisdiction provides sufficient protection. It should be noted that the data does not necessarily have to be stored in one location; it may be split between several locations, change its location depending on operations of the provider or the data may be backed up in several different locations. Therefore it may be difficult to assess this issue thoroughly, nevertheless there should be maximum effort to do so.

Recoverability of stored data

Cloud providers frequently store the data in multiple locations. Thus, in case the servers in one location go down, the data can be either copied or backed up to another data center and can therefore be back in operation in minutes. Choosing a cloud provider with such capability might be preferable.

Cloud provider's uptime

The cloud service is only as valuable as it is accessible. Although the cloud services are relatively stable, the attorney/law firm should always inquire about the provider's uptime and assess whether it's sufficient.

Cloud computing is a valuable resource that provides benefits on a global scale. Cloud technology, if used appropriately, can help reduce costs and increase work efficiency. While there are potential pitfalls when choosing a suitable cloud service, as long as lawyers perform a thorough due diligence and address the above mentioned issues, the benefits of cloud may far outweigh the pain of due diligence. As the number of cloud users is increasing rapidly and the terms of service often differ, there might be a need for a certain level of standardization in order to properly address areas that need specific protection. Standard contracts that would encompass all of the concerns and protections desired may be created as cloud continues to evolve as one of the dominating segments of information technology services.

1 IDC, Quantitative Estimates of the Demand for Cloud Computing in Europe and the Likely Barriers to Uptake, 13 July 2012 Final Report for the European Commission.
2 Among others, it's the improvement of efficiency, greater flexibility, cost reduction and the possibility to access data anytime from anywhere in the world. Furthermore, the immediate sync functionality that allows for immediate access of the most recent version of a document from any device is particularly popular.
3 Secure access, multifactor authentication, encryption and others. The cloud provider should also have sufficient security measures towards its employees and limit their access to stored data in order to minimize risk of offline intrusion techniques such as social engineering and others.
4 The stored data is strictly encrypted so not even the company has a way of accessing it. The server never knows the content of the data being stored.
5 The data is usually located on servers off-site and frequently the cloud providers are renting the storage in "Tier 4" data centers owned by cloud giants such as Amazon, RackSpace or other hosts.