New Jersey Law Journal

VOL. 214 - NO 13 MONDAY, DECEMBER 30, 2013 ESTABLISHED 1878

LEGAL TECH

Consider These Ethical Issues Before Moving Data to the Cloud

A committee with great foresight provided guidance for N.J. attorneys

By Scott E. Reynolds and Harold S. Atlas

Cloud computing offers many advantages, and its use over the past few years has increased dramatically, especially in the area of data storage. The cloud's benefits over traditional data-storage platforms include: minimal capital expenditure, ease of access, transferability, virtually unlimited storage and efficiency. It can be no surprise, therefore, that many law firms have begun the process of transferring vast amounts of data to third-party cloud service providers rather than retaining in-house data centers, which are costly to maintain, require routine software and hardware upgrades and are limited by the amount of available storage.

As cloud computing has gained popularity and become more commonplace in the legal profession, the American Bar Association and state ethics committees across the country have been considering law firms' use of cloud computing to manage and store client documents. Thus far, approximately 14 state ethics committees have considered the issue, directly or indirectly, each coming to the conclusion that law firms may utilize cloud computing to store client information without running afoul of their version of the Rules of Professional Conduct (RPC), so long as certain precautions are taken before entering into a services agreement or master services agreement (MSA) with a cloud service provider. See www.americanbar.org, "Cloud Ethics Opinions Around the U.S."

In an effort to provide further guidance to lawyers regarding the use of technology to store confidential client information, in August 2012, the ABA passed an amendment to model RPC 1.6 to add the following: "A lawyer shall make reasonable efforts to prevent inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."

While New Jersey has not adopted the ABA's proposed amendment to model RPC 1.6, existing RPC 1.15(a) plainly requires attorneys to preserve client property, including documents, for a period of seven years. New Jersey's Advisory Committee on Professional Ethics (Ethics Committee) has not directly addressed whether the use of cloud computing by law firms complies with RPC 1.15. However, on April 10, 2006 (long before cloud computing was popularly known), the Ethics Committee issued Opinion 701, which established guidelines relevant for determining whether cloud computing complies with a lawyer's ethical obligation to preserve client information. 184 N.J.L.J. 171 (Apr. 10, 2006).

In Opinion 701, the Ethics Committee considered whether it is permissible for a law firm to scan and store client documents into digitized format, such as portable data format (PDF), with the exception of certain client documents that, by their very nature, must be maintained physically and in a separate file (e.g., wills). Acknowledging that there is nothing in the RPCs mandating that client documents be archived in a particular format, the Ethics Committee recognized that to the extent new technology enhances an attorney's ability to competently represent her client, "it is a welcome development." Indeed, with considerable foresight, the Ethics Committee considered that:

> It is very possible that a firm might seek to store client sensitive data on a larger file or server or a web server provided by an outside Internet Service Provider (and shared with other clients of the ISP) in order to make such information available to clients, where access to that server may not be exclusively controlled by the firm's own personnel.

Opinion 701 warns, however, that New Jersey attorneys must "exercise reasonable care" when determining the methods used to safeguard confidential client infor-

Reynolds and Atlas are partners at Riker, Danzig, Scherer, Hyland & Perretti in Morristown. Reynolds is a member of the firm's commercial litigation department, and Atlas is a member of the firm's corporate and technology law departments.

mation. Of utmost concern to the Ethics Committee was ensuring that confidential client information is not inadvertently disclosed to third parties. Recognizing that it is already common practice for lawyers to entrust confidential client documents with outside vendors, the Ethics Committee stated that reasonable care must be used to ensure that unauthorized disclosure does not occur when storing client information on third-party servers. A lawyer acts with "reasonable care" where"

> (1) the lawyer has entrusted documents to an outside provider under circumstances in which there is an enforceable obligation to preserve confidentiality and security, and (2) use is made of available technology to guard against reasonably foreseeable attempts to infiltrate the data.

While Opinion 701 provides a good framework for determining whether cloud computing satisfies the RPCs, as cloud computing continues to evolve, recent ethics opinions around the country and technological advancements suggest that there are additional factors law firms should consider before transferring client information to a cloud service provider. Many of these factors should be clearly articulated in the MSA. Below is a nonexhaustive list of important items to consider when selecting a cloud service provider to store confidential client information:

• *Unfettered access to data.* It is critical to ensure that access to client data will not be inhibited. The need for immediate access to client information is at all times vital.

• *Perform due diligence.* Take care to select a provider that has a proven track record working with law firms and understands the unique needs law firms face when storing confidential client information. Also, select a provider that has a strong operating record and a reputation for being financially stable.

• *Data protection.* What methods does the provider employ to secure data maintained in the cloud and during transmission, including the availability of password protection and encryption? How quickly and by what means will you be notified in the event of a security breach? Confirm the provider's backup policies to ensure that they satisfy the law firm's internal policies for maintaining data redundancy over a specified time period.

• *Geographic location of stored data.* Determine if the client information will be stored on servers located outside the United States. Foreign countries have different data protection laws. To avoid complications with respect to data storage, the location or potential location of data storage should be determined from the outset.

• *Ownership of data.* The MSA should plainly state that all data belongs to the user, not the provider.

• *Data retention policy.* Understand the provider's data retention policy to confirm it is consistent with both the law firm's internal requirements to preserve data and those established by applicable professional rules.

• *Litigation hold.* The duty to preserve evidence for pending or reasonably anticipated litigation may extend a law firm's duty to preserve client information beyond RPC requirements. Protocols should be established with the cloud service provider to ensure a prompt and efficient procedure for serving a litigation hold letter and ensuring that the provider strictly complies with its instructions.

• *Termination/Transition.* Determine ahead of time the steps necessary to obtain and/or transfer client information upon termination of the agreement with the cloud service provider. Also, obtain clear guidance on what assistance is provided by the vendor in the event its services are terminated. Termination of services can leave a law firm vulnerable to delays in accessing data and interruption of critical services.

The cloud computing industry is moving quickly. Advancements appear to occur on an almost daily or weekly basis. While Opinion 701 provides a good framework for guiding law firms through the ethical pitfalls of storing client information with cloud service providers, recent advancements in the industry may today require that a law firm be more vigilant to ensure that it has satisfied its obligation to act with "reasonable care" to protect client information. Before entering into a MSA with a cloud service provider, a law firm, like any other business, should consult with counsel experienced in negotiating MSAs with cloud service providers. This will not only ensure that the law firm avoids potential ethical pitfalls associated with contracting with a cloud service provider, but also that the relationship with the provider will be beneficial to the law firm as a business. ■