

MOSES & SINGER LLP

“Cloud Computing: Ethical Shades of Gray”

By Devika Kewalramani

03-21-11

Lawyers have been communicating with their clients through the clouds for years. Firm websites, e-mails and blogs effortlessly and instantaneously connect lawyers to their clients via computers, smart phones and now, tablets. The Internet, propelled by ever-changing and evolving technology, offers borderless accessibility. The most recent manifestation of this phenomenon is "cloud computing." Also known as "software as a service" or SaaS, cloud computing is a form of remote electronic data storage on the Internet. Data stored "in the cloud" are maintained by vendors and stored on large servers that may be located anywhere in the world. Typically, the vendor purchases and maintains its hardware and software, and firms pay a monthly fee to the vendor for its services.

While this form of outsourcing is touted as fostering firm efficiency and cost-saving, the elusiveness of this new type of data storage has raised eyebrows in the legal community as to its ethical propriety. In particular, potential concerns regarding confidentiality, security and control surround cloud computing.

Spearheading an effort to identify specific practical concerns surrounding cloud computing and ways to develop necessary guidelines, the American Bar Association (ABA) Commission on Ethics 20/20 Working Group on the Implications of New Technologies, published an Issues Paper Concerning Client Confidentiality and Lawyers' Use of Technology on Sept. 20, 2010. The issues paper highlighted a number of concerns regarding a lawyer's use of cloud computing, including unauthorized access to confidential client information; storage of information on servers in countries with fewer legal protections; vendor failure to adequately back up data; unclear policies regarding data ownership; policies for notifying customers of security breaches; insufficient data encryption; the necessity for client consent; and policies for data destruction.

The ABA sought public comment from the legal community in late 2010 in response to three non-mutually exclusive options it proposed: (1) white paper/guidance; (2) creation of an online resource; and/or (3) amendments to the Model Rules of Professional Conduct.

Common Concerns

About 10 years ago, it was the emergence of e-mail that prompted concerns within the legal community about the ability to relay client confidences securely and confidentially. The ABA issued a Formal Opinion concluding that lawyers may transmit information relating to client representation by unencrypted e-mail sent over the Internet, without violating Rule 1.6 of the Model Rules, because this mode of transmission "affords a reasonable expectation of privacy from a technological and legal standpoint." (ABA Formal Opinion 99-413 (1999)).

Rule 1.6 prohibits a lawyer from revealing information relating to the representation of a client unless the client gives informed consent or the disclosure is impliedly authorized to carry out the representation. Under the rule, lawyers must act competently to safeguard information relating to client representation and take "reasonable precautions" to protect against inadvertent or unauthorized disclosure.

The same rationale that was applied to e-mail has similarly been extended to cloud computing. Ethics authorities have suggested ways in which lawyers can take reasonable precautions to protect client data stored in the clouds. The first New York ethics opinion to address the ethics of online storing of confidential information was issued last fall by the New York State Bar Association (NYSBA) Committee on Professional Ethics. (NYSBA Opinion 842 (2010)). In addition to the lawyer's own duty of reasonable care, Rule 1.6(c) of the New York Rules of Professional Conduct obligates a lawyer to exercise reasonable care to prevent others whose services are utilized by the lawyer from disclosing or using confidential client information.

Exercising reasonable care does not mean that the lawyer guarantees that the information is secure from any unauthorized access. The Committee on Professional Ethics concluded that lawyers may rely on cloud computing to store client files, as long as the lawyer takes reasonable care to ensure the system is secure and that client confidentiality will be maintained. The Arizona State Bar Association Committee on the Rules of Professional Conduct reached a similar conclusion in its opinion addressing electronic data storage. (AZ Bar Ethics Op. 09-04 (2009)).

Chasing Clouds

The difficulty with the reasonableness standard is that when it comes to technology, what is reasonable is constantly changing. For now, lawyers should strongly consider conducting due diligence before making any decision to dispatch their clients' data to the clouds. For example, lawyers should ensure the online computer data storage provider they use has an enforceable obligation to preserve confidentiality and security, and that the provider will promptly respond to the lawyer or firm if they are required to produce client documents, files or records relating to a transaction or proceeding. In addition, lawyers should investigate the online data storage provider's own security measures, policies, recoverability methods, and related practices and protocols, including its ability to purge copies of data or transfer data to a different host. This information should be provided in the storage provider's terms of service.

Finally, lawyers should employ available technology to guard against reasonably foreseeable attempts to infiltrate properly stored data. This process of course is ongoing. As the technology continues to develop, lawyers must stay current with legal developments and potential risks. In short, the duty of reasonable care now invokes a duty to keep up.

Cloudsourcing

The ABA Commission on Ethics pointed out in its Issues Paper that cloud computing is a form of outsourcing, and has queried whether the procedures it previously outlined on lawyer outsourcing should extend to cloud computing. In 2008, the ABA issued a Formal Opinion addressing a lawyer's obligations when outsourcing nonlegal support services. (ABA Formal

Opinion 08-451 (2008)). The opinion emphasized that under Model Rule 5.3, a lawyer who employs, retains or associates with a nonlawyer must make reasonable efforts to ensure that the person's conduct is "compatible with the professional obligations of the lawyer."

Model Rule 5.3 presents many challenges for lawyers who outsource non-legal work. For example, lawyers must ensure that tasks are delegated to individuals who are competent to perform them and must oversee the execution of the outsourced project satisfactorily and appropriately. These requirements may place a considerable burden on lawyers utilizing cloud computing. For instance, if a lawyer wishes to send confidential client information to a data storage vendor, the lawyer should consider investigating the security of the vendor's network, its backup systems, type of data encryption, and policies regarding retrieval of data upon the termination of services.

Under the Model Rules, lawyers may need to provide information to clients concerning any existing or proposed outsourcing relationships and, in some instances, obtain the client's informed consent to the engagement of a remote data storage vendor. In addition, a written confidentiality agreement between an outsourcing lawyer and the client may be advisable.

Cloud Control: Best Practices

In December 2010, recognized leaders in legal cloud computing announced the establishment of the Legal Cloud Computing Association (LCCA), which is tasked with facilitating adoption of cloud computing technology within the legal profession in accordance with applicable ethics rules. The LCCA has recommended steps that lawyers and law firms can take to protect confidential client information while outsourcing data to the cloud:

- **Confidentiality.** Lawyers and firms should seek information from their data storage providers regarding the identity of persons who have access to the system and data, and whether and under what circumstances the provider's personnel or any third-party business partners are subject to confidentiality obligations.
- **Security.** Lawyers and firms should have a clear understanding of the vendor's security practices, especially in the case of a security breach, as well as its encryption protocols and storage procedures.
- **Control.** Lawyers and firms should ensure that any data they forward to a vendor for uploading to the cloud remain the sole and exclusive property of the firm. In addition, storage providers should be asked to disclose whether they use servers located outside the United States, which may be subject to different laws and regulations.

Cloud computing may have much to offer lawyers and law firms, but it is not without risks. Ethics authorities seem to agree that cloud computing places a heavy load on a lawyer's shoulders to understand and monitor a vendor's practices and to continue to stay on top of technological changes and advancements.

In weighing the benefits and burdens of outsourcing to the cloud, lawyers may want to think about the possibility that certain clients may be better candidates for cloud computing than

others. For example, large institutional client data relating to multi-billion dollar transactions may be more susceptible to hacking than data belonging to a small business or individual client, where the stakes are presumably much lower. In addition, financial services institutions, which are heavily regulated, need to be able to retrieve and produce large quantities of data on demand from regulators.

On the other hand, larger clients may also be more inclined to seek the benefits of cloud computing, since their data storage needs are likely to be greater. In this sense, cloud computing creates an interesting tension between volume and security. Ultimately, it is the lawyer's responsibility to carefully evaluate the risks and rewards of cloud computing, without ever losing perspective...through the clouds.

Devika Kewalramani is a partner and Co-Chair of Moses & Singer's Legal Ethics & Law Firm Practice Group. **Shira L. Auerbach**, a former associate at the firm, assisted in the preparation of this article.

Devika Kewalramani
New York, N.Y.

Reprinted with permission from the "March 21, 2011" edition of the "New York Law Journal" © 2011 ALM Media Properties, LLC. All rights reserved. Further duplication without permission is prohibited. For information, contact 877-257-3382, reprints@alm.com or visit www.almreprints.com.

MOSES & SINGER LLP

Disclaimer

Viewing this or contacting Moses & Singer LLP does not create an attorney-client relationship.

This is intended as a general comment on certain developments in the law. It does not contain a complete legal analysis or constitute an opinion of Moses & Singer LLP or any member of the firm on the legal issues herein described. This contains information that may be modified or rendered incorrect by future legislative or judicial developments. It is recommended that readers not rely on this general guide in structuring or analyzing individual transactions or matters but that professional advice be sought in connection with any such transaction or matter.

Attorney Advertising

It is possible that under the laws, rules or regulations of certain jurisdictions, this may be construed as an advertisement or solicitation.

Copyright © 2011 Moses & Singer LLP
All Rights Reserved