Ethics & Professional Compensation Committee

ABI Committee News

In This Issue **Volume 8, Number 1 / February 2011**

Up in the Cloud: Ethical Issues that Arise in the Age of Cloud Computing

by Patrick Mohan
Barton Law Firm, P.A.; Columbia, S.C.
Steve Krause
Davis Polk & Wardwell LLP; New York

Committee Officers

Upcoming Events

Contribute to the Newsletter

ABI World

Newsletter Archives

Whether it is discovery, pleadings or transactions, lawyers produce enough pages to fill countless file cabinets. As a means of alleviating the cost associated with additional physical storage space, attorneys have turned to digital storage solutions for client files, including confidential information. Unlike physical file cabinets under lock and key that only have to be protected from the elements and physical intrusion, digital storage solutions are complicated by issues of electronic security and the associated risks of breaching clients' basic confidences as well as information protected by the attorney-client and work product privileges. The risk of viruses or hackers infiltrating digital data is greater than ever, as even the use of a personal e-mail account on a firm computer may pose a risk to sensitive client data. Despite these growing threats, many attorneys fail to take the necessary precautions in adopting digital storage solutions that best protect their clients.

What Is the "Cloud"?

Colloquially, the "cloud" is all of the resources available using the Internet. More technically, cloud computing is comprised of an array of domains and servers accessible through a network of Internet service providers,. [1] and includes any service provided online and operated by a third party. [2] The cloud includes:

- online data storage (*e.g.,* Mozy.com, Carbonite.com);
- Internet-based e-mail (*e.g.,* AOL, Yahoo or Gmail); and
- Software as a service ("SaaS"), including law practice management applications that can assist attorneys with conflicts checks, document management and storage, trust-account management, timekeeping and billing. [3]

Comparing Cloud Storage to Offline File Storage

The legal profession has developed many safeguards to protect client confidences. As an individual attorney gives up direct control of his or her client's information, he or she takes calculated risks with the security of that information. First, there is the risk of hiring junior attorneys. What if an associate improperly shares privileged information? Then there is the risk of off-site document destruction. What if the shredding company fails to shred some (or all) documents? There are also risks that arise with the use of off-site file storage. What if the company fails to guard its facility? Another set of potential risks arises from out-sourcing administrative tasks or legal work. In these scenarios, state bar associations and/or legislatures have provided guidance for attorneys in navigating these challenges and provided opinions on managing the cloud.

State Bar Ethics Opinions

State bars have issued opinions considering and authorizing the use of cloud computing. [4] The California and New York bar associations have been frontrunners, each publishing detailed reports outlining attorneys' responsibilities in choosing and using technology.

California: In 2008, the Standing Committee on Professional Responsibility and Conduct for the California State Bar Association [5] considered the implications of the California Code and Rules of Practice [6] on the use of the cloud. Their analysis contrasted the Model Rules of Professional Conduct, California statutes and relevant case law, in addition to accounting for parallels in lower tech approaches (*e.g.,* the mail, telephones, etc.). California concluded that the standards of lawyer competence require lawyers to apply the same sorts of safeguards in the online world that they would offline. For instance, e-mails should be considered as likely to be misdelivered or intercepted as postal mail, and thus appropriate, but not extreme, care should be taken with e-mail. Moreover, attorneys have an obligation to reasonable precautionary measures to increase the security of confidential client information. Taking a realistic approach that should comfort the luddites among us, the California Bar did not require that attorneys understand the technology they use: The requirement is simply to understand one's own limitations and seek appropriate counsel and advice with respect to any such technology. Finally, the California Bar cautioned attorneys to heed their client's requests and not use any technology the client specifically rejects.

New York: The New York State Bar Association has also reached similar conclusions, stating that it is reasonable for lawyers to use the "cloud" as long as they take reasonable care in how they use it. New York maintains that attorneys have the obligation to confirm that the technology is adequately protecting client confidences and that its providers continue to take reasonable measures to prevent unauthorized access to client data and allow the data to be deleted or moved upon the lawyer's request. Significantly, New York also requires attorneys to notify their clients in the event of a breach.

Although it has not yet issued a formal opinion, the American Bar Association (ABA) Commission on Ethics recently weighed-in on cloud computing as well. [7] The ABA recently solicited feedback on the issue and is mulling its next steps. In the meantime, the commission has provided some commentary on considerations for attorneys contemplating the use of the cloud. Furthermore, the ABA is considering whether cloud computing constitutes outsourcing and thus implicates Model Rule of Professional Conduct 5.3 governing the supervision of nonlawyers and, if so, how that rule should be amended. The ABA is also considering whether particular requirements should be imposed on the use of the cloud and whether the industry standards are appropriate.

Navigating through the Cloud

Of course, the issues lawyers should consider when working within the cloud include:

- How sensitive are the documents in question?
- Who will have access to these documents in the cloud?
- What happens if these documents are not maintained securely?
- What can I do to improve the security of my clients' files on the cloud?
- Is this solution going to be cost-efficient?

More significantly, in addition to ethics opinions, several bar associations have created lists of questions that lawyers should be prepared to ask of potential service providers. Based on our review of these questions, there are a few key topics that every lawyer must ask before putting client files in the cloud.

Security

- Are the company's employees adequately screened, trained, etc.?;
- Can the company's employees access documents?;
- How secure is the electronic encryption, both in transmission and in storage?
- Are the physical premises hosting the data secure?

- What happens if data is improperly accessed, and what is the notification process?
- Who owns the premises, the servers, and even the data?
- Where will data storage be located?
- How is data destruction handled?

Backups

- How often are servers backed up?
- How long are backups saved?
- Are backups verified?
- How often are files backed up?
- Are backups stored off-site?
- Can data be improperly accessed electronically during backup?
- Is the off-site backup physically secure?
- What happens if data is lost?
- Where will backup data be located?

Service Continuity

- What amount of downtime is permissible or acceptable?
- What happens to my data if there is a service interruption?
- What if the provider is sold, goes out of business or files for bankruptcy?

In addition to the questions provided above, lawyers should consider certain additional measures that may be available. As an added precaution, attorneys should review activity reports. Just as Westlaw can provide a research trail, and credit cards and banks provide statements, there is no reason that digital storage providers cannot provide activity reports. These reports should identify who has accessed client information, when it was accessed and what files were viewed. This protects not only privileged information but also the more basic client right to confidentiality.

Conclusion

As evidenced by the growing number of digital storage solutions that are being advertised in bar announcements and legal publications, not to mention to broader non-legal audiences, the cloud is here to stay. It presents a cost-effective storage

solution, but also creates risks to the security of confidential client information. With proper due-diligence and reasonable care, attorneys can avoid the ethical pitfalls of cloud computing and experience all the benefits cloud computing has to offer for their firms and clients.

1. *See* ABA Commission on Ethics 20/20, Sept. 20, 2010, www.abanet.org/ethics2020/pdfs/clientconfidentiality_issuespaper.pdf (last visited Dec. 8, 2010).

2. *Id.*

3. *Id.*

4. *See, e.g.,*State Bar of Ariz. Op. 09-04 (2009), State Bar of Ariz. Op. 05-04 (2005), Cal. State Bar Form. Op. Interim 08-0002 (2008), Fla. Bar Op. 06-01 (2006); Ill. State Bar Ass'n Op. 96-10 (1997), Maine Prof'l Ethics Comm'n Op. no. 194 (2008), N.C. State Bar Proposed Formal Eth. Op. 2010-7 (Apr. 15, 2010), N.Y. State Bar Op. 842 (Sept. 10, 2010), N.J. Supreme Court Advisory Comm. on Prof'l Ethics, Op. 701 (Apr. 10, 2006), Nev. State Bar Standing Comm. on Ethics & Prof'l Responsibility, Formal Op. 33 (Feb. 9, 2006), State Bar Ass'n of N. Dak. Op. 99-03 (1999), Penn. Bar Ass'n Op 2005-105 (2005), Vermont State Bar Opn. 2003-03 (2003).

5. The State Bar of California's Standing Committee on Professional Responsibility and Conduct issued a new formal opinion finalizing its assessment of the impact of the use of technology on an attorney's duties of confidentiality and competence to a client. Cal. State Bar Form. Op. 2010-179 (2010).

6. Rules 3-100 and 3-110 of the Rules of Professional Conduct and California Code § 6068(e)(1).

7. ABA Comm. on Ethics and Prof'l Responsibility, Issue Paper Concerning Client Confidentiality and Lawyers' Use of Technology," Sept. 20, 2010, www.abanet.org/ethics2020.