Cloud Computing — A Silver Lining or Ethical Thunderstorm for Lawyers?

by James M. McCauley, Ethics Counsel, Virginia State Bar

Because of the flagging economy, businesses and professionals are searching for increased efficiency and reduced costs and risks in their endeavors. This is especially true for the ever-increasing risks and costs associated with information technology (IT) management. Today, the business world is overrun with entreaties by IT firms offering "cloud computing services" who advertise that "the future is here and it is in the clouds."

What Is Cloud Computing?

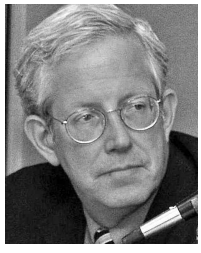
There is no one agreed definition of "cloud computing."[1] Software as a Service (SaaS) is but one form of cloud computing referring to a category of software delivered via the Internet to a web browser (such as Internet Explorer) rather than installed directly onto the user's computer. The resulting data is held by the third-party service provider (or maybe by a data center provider by companies like Amazon, RackSpace or other host), not on a computer or server within the law firm. Cloud computing is not new, but it has become a hot topic in the IT and business world. Software has been employed over networks for decades, including through application service providers that rose to prominence in the 1990s and then fizzled out with other tech companies that went bust in the early 2000s. Some lawyers already use web-based applications in their practice, including online legal research (Westlaw, LexisNexis, CaseFinder or Fastcase), web-based e-mail (Gmail, Yahoo, or Hotmail), document creation or collaboration tools (Google Docs), and data backup services (Mozy, i365, IBackup, Steel Mountain, and Carbonite). These are all examples of cloud computing. Although the concept of cloud computing is not new, its rapid expansion and diversification in the IT and business world are recent.

Cloud computing might also be described as shifting information technology responsibility from the consumer to service providers who deliver IT services via the Internet — the "cloud." The consumer relinquishes control over IT functions compared with legacy systems. Responsibility shifts from the consumer to a third party for infrastructure, application software, development platforms, developer and programming staff, licensing and updates, security, and maintenance. Some might describe cloud computing as the virtualization of the computing process or as outsourcing IT.[2]

Many firms today are considering switching from obtaining and loading software on their own computers to SaaS platforms to facilitate their practices, particularly in the areas of case management and time and billing platforms. There are arguments for and against using SaaS. Examine those issues before you decide to switch over. Cloud computing liberates the consumer from many of the burdens of IT management issues, enabling the consumer to focus on core activity. Cloud computing also reduces costs and expenses associated with purchasing and maintaining the hardware and software necessary to run applications, security measures, backup, and disaster recovery.

Benefits of Cloud Computing

- **Save money:** Cloud computing applications greatly reduce the costs of electronic data management. These applications are less expensive than designing your own program or modifying an existing program. Focus your technology budget on competitive advantage rather than infrastructure.
- **Identified cost:** Your investment in hardware and software is minimized. Cost for the SaaS model can be based on the number of users or the amount of data storage volume; it is easy to identify and budget for monthly or annually. For the best pricing, the contract terms are often multiyear commitments — sometimes three to five years.
- **Save time:** There is no installation, and the SaaS provider takes care of updates, including security, and is responsible for data storage and retrieval.
- **Intuitive:** SaaS programs are more intuitive and easier to use than traditional software. However, because they



James M. McCauley is the ethics counsel for the Virginia State Bar. He and his staff write the draft advisory opinions for the Standing Committees on Legal Ethics and Unauthorized Practice of Law and provide informal advice to members of the bar, bench, and general public on lawyer regulatory matters, through the Legal Ethics Hotline (http://www.vsb.org/site/regulation/ethics/). McCauley teaches professional responsibility at the University of Richmond School of Law in Richmond and serves on the American Bar Association's Standing Committee on Legal Ethics and Professionalism.

are newer, they sometimes have more limited features than older software programs.

- **Staying current:** Gain immediate access to the latest innovations and updates at the provider's expense.

- **Mobility:** SaaS products allow lawyers to access their software and their data from many locations, without additional cost (with an Internet connection). Because most SaaS is accessed through a web browser, system requirements are minimal.

- **Service:** You may get better service from a vendor. If you are considering SaaS, ask a vendor about a service level agreement. A good agreement should guarantee both a certain level of uptime for the product and a response time for technical and support service requests.

Ethical Concerns for Lawyers Using Cloud Computing

Concerns about Security and Reliability. There are always concerns about a new technology's security and reliability. Comment 16 to American Bar Association Model Rule 1.6 states that "[a] lawyer must act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are under the lawyer's supervision." Comment 17 states that "the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients."

There is no basis in the Virginia Rules of Professional Conduct for an unqualified prohibition of lawyers managing their office software applications and client data using cloud computing. Lawyers have always had an ethical duty to safeguard confidential client information. Rule 1.6. However, lawyers may share information protected under Rule 1.6 with third parties as needed to perform necessary office management functions, if the lawyer exercises reasonable care in the selection of the third-party vendor and secures an agreement that the vendor will safeguard the confidentiality of the information shared. Va. Rule 1.6(b)(6). In the past, lawyers have outsourced copying and document production to third-party vendors. Confidentiality of client information was protected by contractual arrangements between the law firm and the third-party vendor. In other advisory opinions, the VSB Standing Committee on Legal Ethics has emphasized that lawyers must act competently to protect the confidentiality of information relating to the representation of their clients, including protecting both open and closed client files.[3]

In ABA Formal Opinion 95-398 (1995) the American Bar Association's Standing Committee on Legal Ethics and Professionalism recognized that "in this era of rapidly developing technology, lawyers frequently use outside agencies for numerous functions such as accounting, data processing, photocopying, computer servicing, storage and paper disposal and that lawyers retaining such outside service providers are required to make reasonable efforts to prevent unauthorized disclosures of client information." The opinion states that outside service providers would be considered to be nonlawyer assistants under Model Rule 5.3, which states that lawyers have an obligation to ensure that the conduct of the nonlawyer employees they employ, retain, or become associated with is compatible with the professional obligations of the lawyer. But how does a lawyer exercise the supervision required of Rule 5.3 over a company such as Google or Yahoo that essentially offers cloud computing contracts on a take-it-or-leave-it basis?

In addressing attorney use of the Internet for client file storage, the State Bar of Arizona's Ethics Committee has stated:

> [A]n attorney or law firm is obligated to take reasonable and competent steps to assure that the client's electronic information is not lost or destroyed. In order to do that, an attorney must be competent to evaluate the nature of the potential threat to client electronic files and to evaluate and deploy appropriate computer hardware and software to accomplish that end. An attorney who lacks or cannot reasonably obtain that competence is ethically required to retain an expert consultant who does have such competence. Arizona State Bar Op. 05-04.

The Massachusetts Bar Association Committee on Professional Ethics issued an ethics opinion that "A law firm may provide a third-party software vendor with access to confidential client information stored on the firm's computer system for the purpose of allowing the vendor to support and maintain a computer software application utilized by the law firm. … However, the law firm must 'make reasonable efforts to ensure' that the conduct of the software vendor (or any other independent service provider that the firm utilizes) 'is compatible with the professional obligations of the lawyer[s],' including the obligation to protect confidential client information reflected in Rule 1.6(a). The fact that the vendor will provide technical support and updates for its product remotely via the Internet does not alter the Committee's opinion." Massachusetts Bar Op. 2005-04 (March 3, 2005).

Attorneys are not required to guarantee that a breach of confidentiality cannot occur when using an outside service provider. Rule 1.6 only requires the lawyer to act with reasonable care to protect information relating to the representation of a client. Nevada's Ethics Committee addressed the question of whether an outside party could be used to store files in digital format or if this would be considered a breach of confidentiality. In reaching a decision, the Nevada committee analogized storing digital files on an off-site server to storing paper documents in an off-site storage facility operated by a third party. In reviewing prior ABA opinions, the committee concluded that as long as the lawyer exercises care in the selection of the vendor, has a reasonable expectation that the vendor will keep the data confidential and inaccessible by others, and

instructs the vendor to preserve the confidentiality of the information, the requirements of Rule 1.6 are met. Nevada Formal Op. 33 (2006).

A recent Alabama ethics opinion takes a similar approach consistent with the Nevada and Arizona opinions. Alabama lawyers may outsource the storage of client files using cloud computing if they keep abreast of appropriate security safeguards and take reasonable steps to make sure the off-premises provider uses sound methods to protect the data. Alabama State Bar Disciplinary Comm'n, Op. 2010-02.

Although Virginia has not issued an ethics advisory opinion on a lawyer's use of cloud computing, Virginia Rule 1.6(b)(6) appears similar to Alabama's. The rule allows lawyers to share confidential information with an outside agency if "necessary for statistical, bookkeeping, accounting, data processing, printing, or other similar office management purposes, provided the lawyer exercises due care in the selection of the agency, advises the agency that the information must be kept confidential and reasonably believes that the information will be kept confidential." This rule does not require the lawyer to obtain the client's consent before disclosing information to the outside agency. In LEO 1818 (2005) the Virginia State Bar's Standing Committee on Legal Ethics concluded that a lawyer or law firm may store a client's file or information in electronic or digital format. In so doing, the committee acknowledged in a footnote that it may be necessary for the lawyer to rely on outside technical support to develop a paperless office.[4]

If you are using a SaaS provider, protect your confidential data and information. Secure portals and secure transmission protect client confidentiality. Is the transmission of the data encrypted to preserve confidentiality? Are you using a safe password or even biometrics for access?

Laws Protecting Privacy of Data

Laws in the United States and overseas protect privacy of data or information. They include the Family Educational Rights and Privacy Act of 1974; the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996), 42 U.S.C. 1320d et seq., 45 C.F.R. Parts 160 & 164; and the Gramm-Leach-Bliley Act, 15 USC 6801et seq. Various states may have data protection or security laws, such as Massachusetts General Law Chapter 93H, Regulations 201 CMR 17.00; the New Jersey Identity Theft Protection Act, N.J.S.A. 56:11-44 to 50 and 56:8-161 to 166; and the Virginia Health Records Privacy Act, Va. Code § 32.1-127.1:03.

The Federal Trade Commission has posted enforcement actions for security breaches by cloud computing providers.[5] The European Union also has laws protecting the privacy of information that may affect users of cloud computing.[6]

There has been much discussion in the legal community over whether lawyers should convert to SaaS. Opponents argue that lawyers should not be the first to test the water. Rather, lawyers should consider letting problems be resolved by other businesses. Lawyers should protect of their data and their clients' data. Putting it in the hands of a third party is a loss of control that should not be risked. On the other hand, proponents of SaaS say that lawyers have shared client information with third-party vendors for decades and that data stored in the cloud is at least as safe and secure, if not more so, than data stored locally. They argue that most SaaS vendors use sophisticated data centers to house their customer's data. These data centers feature elaborate, redundant security and backup systems to ensure that data is protected from accidental loss and unauthorized access. The technology and the expertise employed by SaaS vendors are greater than at most law firms. Carefully consider the pros and cons before you decide what's right for your firm and your clients.

Because of the complexity of this ever-changing technology, lawyers have to be careful with cloud computing. The primary concern for most is control over the data. While the customer owns the data, the data is stored on a third-party server, the location of which may not be known to the customer. The cloud computing service provider may move the data for its own reasons to another server in another country.

Questions You Need Answered

Cloud computing is a global undertaking. Considerations should include:

- Where will users be located?
- Where will the data be processed?
- Where will the data be stored?
- Where is the disaster-recovery and backup site located?
- Where are the data subjects located?
- Where will support services be based, and will support have access to sensitive data?
- Will subcontractors or outsourcing be utilized for any functions having access to sensitive data?
- Does the customer have the right to approve in advance any transfer of data to another state or country?
- Who will have access to the data and will there be different levels of access?
- Who will supervise the project and will there be monitoring and auditing of policies and procedures?

To see how some of these questions are addressed by Google, you might check out Google's cloud computing contract. A Google Apps Premier Edition Online Agreement can be found at http://www.google.com/apps/intl/en/terms/education_terms.html.

Best Practices for Cloud Computing Vendors

- **Transparency**: Cloud computing platforms should explain their information handling practices and disclose the performance and reliability of their services on their public web sites.
- **Use limitation:** A cloud provider should claim no ownership rights in

customer data and should use customer data only as its customers instruct or to fulfill contractual or legal obligations.

- **Disclosure**: A cloud provider should disclose customer data only if required by law and should provide affected customers prior notice of any compelled disclosure.

- **Security management system:** A cloud provider should maintain a robust security management system that is based on an internationally accepted security framework (such as ISO 27001) to protect customer data.

- **Customer security features:** A cloud provider should provide customers with configurable security features to implement in their usage of the cloud computing services.
- **Data location:** A cloud provider should tell customers the countries in which customer data is hosted.

- **Breach notification:** A cloud provider should notify customers of known security breaches that affect the confidentiality or security of the customer data.

- **Audit:** A cloud provider should use third-party auditors to ensure compliance with its security management system.

- **Data portability:** A cloud provider should make available to customers their data in an industry-standard, downloadable format.

- **Accountability:** A cloud provider should work with customers to designate appropriate roles for privacy and security accountability.

Data May Be Subject to E-Discovery Rules

A client's data may be subject to discovery in pending or anticipated litigation; a lawyer may be ethically obligated to take measures reasonably necessary to preserve client data and avoid spoliation claims. Rule 3.4(a) provides that [a] lawyer shall not:

> (a) Obstruct another party's access to evidence or alter, destroy or conceal a document or other material having potential evidentiary value for the purpose of obstructing a party's access to evidence. A lawyer shall not counsel or assist another person to do any such act.

Rule 3.4(e) requires a lawyer "to make reasonably diligent effort to comply with a legally proper discovery request by an opposing party."

In dealing with cloud providers, lawyers must consider issues regarding access to data, contractual provisions for disclosure of confidential information including customer data to third parties, including via subpoena or other compelled disclosure, and litigation holds may require nondestruction of cloud provider records and backup media.

Conclusion

With any emerging technology, lawyers must confront ethical issues that arise when the lawyer considers using that new technology. Because data security is the lawyer's primary concern, lawyers need to approach the issue of cloud computing carefully. "When going to the cloud, you've got to do some due diligence," to ensure not only that the provider can do what you need it to do, but that it will be around long enough to do it when you need it.[7] Finally, lawyers should consider that there may be particular types of information too valuable or critical to store in the cloud. As David Cearley put it, "I wouldn't ever put the formula for Coca-Cola in the cloud."[8]

Endnotes:

1 For a very technical and detailed definition see the National Institute of Standards and Technology's "NIST Definition of Cloud Computing," authors: Peter Mell and Tim Grance, Version 15, 10-7-09, at http://csrc.nist.gov/groups/SNS/cloud-computing/, last updated Aug. 27, 2010.

2 Kevin F. Brady, "Cloud Computing: Panacea or Ethical 'Black Hole' for Lawyers," *The Bencher*, Nov.-Dec. 2010 at 17.

3 Virginia LEO 1305 (lawyers must destroy and cannot simply dump closed client files). Also, this obligation of confidentiality survives the death of the client. *See* Virginia LEO 1207 (1989). In addition, lawyers may convert paper files into electronically stored data. LEO 1818 (2005).

4 Va. Legal Ethics Op. 1818 (2005) at n.2.

5 ChoicePoint – settlement of data security breach charges in violation of Fair Credit Reporting Act and Federal Trade Commission Act. The settlement included $10million in civil penalties — the largest in FTC's history — and further required $5 million for consumer redress as well as implementation of new procedures. *See* http://www.ftc.gov/opa/2006/01/choicepoint.shtm; and recently filed complaint with the FTC: *IMO Google Inc. and Cloud Computing Services*, seeking injunctive relief and investigation into Google Inc. and its provision of cloud computing services alleging failure to adequately safeguard confidential information)(Complaint available at http://epic.org/privacy/cloudcomputing/google/ftc031709.pdf.)

6 (a) European Union Directive on Data Protection, effective October 1998 (Directive 95/46/EC), prohibits transfer of personal data to non-EU countries if they do not meet EU "adequacy standard" for protection of privacy.

(b) Swiss Federal Act on Data Protection regulates the processing of data about physical and legal persons

(c) Various EU member s may implement their own data protection laws, e.g., German data protection authorities issued April 29, 2010, resolution requiring additional diligence when transferring data to parties who are self-certified under the Safe Harbor program; data protection authority of the German federal state of Schleswig-Holstein issued a June 18, 2010, legal opinion concluding that clouds outside of the EU are unlawful, even if the EU commission has issued an adequacy decision in favor of that country.

7 John Tomaszewski, general counsel of TRUSTe, an Internet privacy services provider in San Francisco, who was a panelist speaking at a presentation titled

Cloud continued on page 54

Cloud continued from page 52

"The Real Realities of Cloud Computing: Will the Cloud Produce Smooth Sailing or Stormy Weather?" on Aug. 7, 2010, offered by the American Bar Association Section of Science and Technology Law. Participants in the program looked at security risks to law firms that choose to move data application and storage into the cloud of the Internet.

8 David W. Cearley, a vice-president at the technology research company Gartner Inc., in Stamford, CT, who was a copanelist at the program cited in note 8, *supra*.

Attorneys May Submit Ethics Questions by E-mail

The Virginia State Bar now responds to lawyer's ethics questions submitted by e-mail, as well as telephone.

E-mail:
Go to http://www.vsb.org/site/regulation/ethics/ and click the blue box, "E-mail Your Ethics Questions."

Phone:
Call (804) 775-0564 and leave a voice mail. Your call will be returned.

The ethics staff tries to respond to questions on the same business day they are received.