Mar 19th, 10:45 AM - 11:45 AM

Ethics on the Wing: Examination of Opinions on Electronic Services and Cloud Computing

Sharon Bradley
University of Georgia School of Law Library, bradleys@uga.edu

Ethics on the Wing: Examination of Opinions on Electronic Services and Cloud Computing

Sharon Bradley, J.D., M.L.S.
Special Collections Librarian
Alexander Campbell King Law Library
University of Georgia School of Law
Athens, Georgia

Ethics on the Wing: Examination of Opinions on Electronic Services and Cloud Computing

Sharon Bradley
University of Georgia School of Law
Athens, Georgia

TABLE OF CONTENTS

I. Introduction

In the aftermath of the 9/11 attacks, many law firms became concerned about maintaining electronic copies of client files. Should they do so as a back-up and what kind of access was needed? Generally state bars adopted opinions that did not require lawyers to create electronic copies but if they did the files had to have adequate safeguards to protect client confidentiality and the security of unique items or materials that could not be reproduced. Online back-up services became popular. These were not active files so to speak but could be retrieved if necessary. They were not intended to be “working” files. In those simpler days files could be copied to discs or external hard drives and stored off-site. Control was maintained by the lawyer.

A decade later and lawyers can operate their entire practice remotely using reasonably priced web-based tools and applications. All active and archived documents can be stored securely on remote servers. They are practicing in the clouds.

II. Cloud Computing

Computer scientist John McCarthy is credited with connecting computers and clouds. At a 1961 program at MIT he fantasized that "computation may someday be organized as a public utility.”[1] A component of cloud computing is Software as a Service (SaaS). In this software distribution model applications are hosted by a vendor or service provider and customers access applications, software,

[1]Architects of the Information Society, Thirty-Five Years of the Laboratory for Computer Science at MIT, Edited by Hal Abelson.

platforms, services, and data over a network. You can use traditional desktop computers or a variety of mobile devices. Your "computer" no longer needs to have large hard drives to hold your applications and documents because they are now held in the cloud.

Email services like Hotmail and Gmail are good examples of cloud services. All of your messages and folders exist on a remote server, not on your computer. The advantages to the cloud include:

- Do not have to buy periodic upgrades. The service provider keeps the service current and makes it work with new and improved browsers.
- Do not have to send the IT staff to every computer to install upgrades.
- Everyone has access to everything from everywhere, attorneys can work from multiple sites.
- There are many free services.

Google Docs is one of the best known free services. Google Docs is not as sophisticated as Word but for most users performing most tasks it is good enough. In addition to being free it is accessible from any Internet connected device. Your documents are always available. Facebook and Flickr are cloud services.

Disadvantages to cloud services include:

- Many services have transactional, monthly, or yearly costs.
- Everyone has access to everything from everywhere. Not all employees need total access.
- A target for hackers. The developers and service providers encrypt their data, but every few months there is a news story about big company databases being compromised.
- Loss of access; if your internet connection is down, you are without email or much else.[2]
- In the cloud you don't actually know where your documents are. It may be difficult to trace the location where the service provider actually stores your documents.

---

[2]You can download your messages and folders and work "offline" or "locally" but that is a different issue.

For lawyers cloud computing raises concerns associated with entrusting a third party with confidential client information. Rule 1.6, Confidentiality of Information, of the Model Rules of Professional Conduct imposes the obligation to protect client confidence. Those states with ethics opinions concerning the use of cloud services stress the importance of taking reasonable care to protect a client's confidential information.

III. State Bar Opinions

Let's review the recent bar ethics opinions regarding electronic storage and access to client records. They are discussed in reverse chronological order. You can access the full text of the opinions at our research guide *Georgia Bar CLE 2012*, libguides.law.uga.edu/cle2012, under the "Cloud Ethics" tab.

North Dakota - Opinion 99-03, June 21, 1999

The ethics committee identified two separate confidentiality issues: 1) transmission of data over the Internet, and 2) the storage of electronic data. The committee concluded that the transmission of data and the use of online data backup services are permissible provided the lawyer ensures adequate security, including limiting access only to authorized personnel and requiring passwords. Who would have predicted that North Dakota would lead the way in approving online storage.

Vermont - Advisory Ethics Opinion 03-03, 2003

In an advisory opinion, the ethics committee concluded that a lawyer may use third-party vendors as consultants for confidential client database recovery if

the vendor fully understands and accepts the clearly communicated confidentiality rules. The lawyer has to make his own determination if the vendor has sufficient safety measures to protect information. A significant breach obligates the lawyer to disclose the breach to the client.

Massachusetts - Opinion 05-04, March 3, 2005

A law firm uses a third-party vendor to maintain its integrated document management application. In order to provide technical support and updates the vendor needs periodic access to the firm's network which means they would have access to client files. The law firm's clients are deemed to have "impliedly authorized" the firm to make their confidential information accessible to the vendor in order to permit the firm to provide representation. The law firm must take reasonable actions to make sure the conduct of the software vendor, or any other independent service provider for that matter, is compatible with all professional obligations, particularly the obligation to protect confidential client information.

Arizona - Opinion 05-04: Electronic Storage; Confidentiality, July 2005

The inquiring attorney was concerned about his obligations to protect electronic files from theft, inadvertent disclosure, and loss or destruction. The ethical rules require that an attorney act competently to safeguard client information and confidences. It is not unethical to store electronic information on computer systems whether or not those same systems are used to connect to the Internet. The lawyer is obligated to take reasonable precautions to assure that the client's confidences are not disclosed to third parties through theft or inadvertence

and to assure that the client's electronic information is not lost or destroyed. To meet that obligation, a lawyer must either: 1) have the competence to evaluate the nature of the potential threat to the client's electronic files and to evaluate and implement appropriate computer hardware and software to reduce the threat; or 2) if the attorney lacks or cannot reasonably obtain that competence, to retain an expert consultant who does have such competence.

Virginia - Opinion 1818, Sept. 03, 2005

Due care was required in selecting a service provider for technical assistance and support for electronic storage.

Nevada - Formal Opinion No. 33, Feb. 9, 2006

The ethics committee revised the original question to more "broadly address the lawyer's duty of confidentiality with respect to electronic client information." Does an attorney violate court rules by "storing confidential client information and/or communications, without client consent, in an electronic format on a server or other device that is not exclusively in the lawyer's control." A lawyer must act competently and reasonably to prevent the accidental and unauthorized disclosure of client information. The lawyer may use an outside agency to store confidential client information in electronic forms, and on hardware located outside the attorney's direct supervision and control, so long as the attorney observes the usual obligations applicable to such arrangements for third-party storage services. If, for example, the attorney does not reasonably believe that the confidentiality will be preserved, or if the third-party declines to agree to keep the information confidential, then the attorney violates ethical rules by transmitting the data to the

third-party. But if the third-party can be reasonably relied upon to maintain the confidentiality and agrees to do so, then the transmission is permitted by the rules even without client consent.

Florida - Opinion 06-1, April 10, 2006

A lawyer may use electronic filing provided that reasonable precautions are taken to ensure confidentiality of client information, especially if the lawyer relies on third parties to convert and store paper documents to electronic records.

New Jersey - Opinion 701: Electronic Storage and Access of Client Files, April 10, 2006

The inquiring attorney wanted to implement an electronic filing system in which all documents received in the office would be scanned into the PDF format. He did acknowledge his responsibility to retain certain documents like wills and deeds in their original hardcopy. When using any kind of third-party service provider it must be under circumstances in which the outside party is aware of the lawyer's obligation of confidentiality. The service provider must agree, by contract, professional standards, or otherwise, to assist in preserving the confidentiality. Lawyers have long used messengers, delivery services, document warehouses, or other service providers, in which physical custody of sensitive documents is entrusted to them even though they are not employed by the firm. The lawyer's duty of care has not changed just because the method of transmission has changed.

Maine - Opinion 194: Client Confidences: Confidential firm data held electronically and handled by technicians for third-party vendors, June 30, 2008

With appropriate safeguards, an attorney may utilize transcription and

computer server backup services remote from both the lawyer's physical office and the lawyer's direct control or supervision without violating the attorney's ethical obligation to maintain client confidentiality. In view of the changing use of evolving technology the committee could not delineate acceptable and unacceptable practices. At a minimum, the lawyer should take steps to ensure that the company providing transcription or confidential data storage has a legally enforceable obligation to maintain the confidentiality of the client data involved.

New York - Opinion 820, Feb. 8, 2008

The obligation to preserve client confidentiality does not preclude using an email service provider that conducts computer scans of emails to generate computer advertising. The question clearly describes free email services such as Gmail and Hotmail. The service provider's privacy policies stated that the emails are not reviewed by or provided to other individuals. The generation of advertising based on scans of the emails posed no greater risk to client confidentiality than email services without the feature.

Illinois - Opinion 10-01: Confidentiality: Law firm's use of a third-party technology vendor, July 2009

A lawyer may use an off-site network administrator to assist in the operation of the office if reasonable efforts are made to ensure the protection of confidential client information.

Arizona - Opinion 09-04: Confidentiality; Maintaining Client Files; Electronic Storage; Internet, Dec. 2009

The question indicates the technical knowledge of the attorney: may the lawyer maintain an encrypted online file storage and retrieval system for clients in

which all documents are converted to password-protected PDF format and stored in online folders with unique, randomly-generated alpha-numeric names and passwords? The lawyer's system of encryption and multi-layers of random folder names and passwords satisfied the obligation to take reasonable precautions. The committee did note that reasonable precautions today may not be reasonable tomorrow and the lawyer also had the obligation to conduct periodic reviews of the security precautions.

New York - Opinion 842, Sept. 10, 2010

The New York opinion is the first to use the word cloud. "Various companies offer online computer data storage systems that are maintained on an array of Internet servers located around the world. (The array of Internet servers that store the data is often called the 'cloud.')" A lawyer may use an online data storage system to store and back up client confidential information provided that the lawyer takes reasonable care to ensure that confidentiality is maintained in a manner consistent with the lawyer's ethical obligations. The lawyer should stay abreast of technological advances to ensure that the storage system remains sufficiently advanced to protect the client's information, and the lawyer should monitor the changing law of privilege to ensure that storing information in the "cloud" will not waive or jeopardize any privilege protecting the information.

Alabama - Opinion 2010-02: Retention, Storage, Ownership, Production and Destruction of Client Files, Dec. 2010

The disciplinary commission came to the now standard conclusion that an attorney must exercise reasonable care in storing client files, which includes

becoming knowledgeable about a provider's storage and security and ensuring that the provider will abide by a confidentiality agreement. Lawyers should stay on top of emerging technology to ensure security is safeguarded. Attorneys may also need to back up electronic data to protect against technical or physical impairment, and install firewalls and intrusion detection software.

California - Formal Opinion 2010-179: Confidentiality and Technology, Jan. 20, 2011

An attorney using public wireless connections to conduct research and send e-mails should use precautions, such as personal firewalls and encryption, or risk violating professional obligations of confidentiality and competence. Some highly sensitive matters may necessitate discussing the use of public wireless connections with the client or in the alternative avoiding their use altogether. Appropriately secure personal connections meet a lawyer's professional obligations. Ultimately, the committee found that attorneys should: 1) use technology in conjunction with appropriate measures to protect client confidentiality, 2) tailor such measures to each unique type of technology, and 3) stay abreast of technological advances to ensure those measures remain sufficient.

Iowa - Opinion 11-01: Use of Software as a Service – Cloud Computing, Sept. 9, 2011

The Iowa opinion was the first to use the phrase "software as a service" (SaaS). The committee discussed Comment 17 to Iowa's Rule 32:1.6:

> When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable

> expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this rule.

The rule seemed reasonable and flexible in helping a lawyer evaluate and use constantly changing technology. It recognizes that the degree of protection to be afforded client information varies with the client, matter, and information involved. But it places on the lawyer the obligation to perform due diligence to assess the degree of protection that will be needed and to act accordingly.

Oregon - Formal Opinion No. 2011-188: Information Relating to the Representation of a Client: Third-Party Electronic Storage of Client Materials, Nov. 2011

Lawyers may contract with third-party service providers to store client files and documents on remote servers so that the lawyer and the client can access the documents over the Internet from remote locations. The lawyer must take reasonable steps to ensure that the storage company will reliably secure client data and keep information confidential. Under certain circumstances, this may be satisfied through a third-party vendor's compliance with industry standards relating to confidentiality and security, provided that those industry standards meet the minimum requirements imposed on the lawyer by the rules of professional conduct. This may include, among other things, ensuring the service agreement requires the vendor to preserve the confidentiality and security of the materials. It may also require the vendor notify the lawyer of any unauthorized

third-party access to the materials. The lawyer should also investigate how the vendor backs-up and stores its data and metadata to ensure compliance.

Pennsylvania - Formal Opinion 2011-200: Ethical Obligations for Attorneys Using Cloud Computing/Software as a Service While Fulfilling the Duties of Confidentiality and Preservation of Client Property, Nov. 23, 2011

The ethics committee concluded that lawyers may ethically allow client confidential material to be stored in "the cloud" provided the lawyer takes reasonable care to assure that: 1) all such materials remain confidential, and 2) reasonable safeguards are employed to ensure that the data is protected from breaches, data loss, and other risks. This opinion considers both the practical and technology-related issues that are raised when lawyers use cloud-based services. To determine reasonable care the committee included a thorough checklist of questions to ask and information to gather. There is a strong emphasis on lawyers being ultimately responsible for making informed decisions about the benefits and risks of placing client data in the cloud. The storing of client data can be outsourced, but the responsibility for making sure it is safe and secure remains with the lawyer.

North Carolina - 2011 Formal Ethics Opinion 6: Subscribing to Software as a Service While Fulfilling the Duties of Confidentiality and Preservation of Client Property, Jan. 27, 2012

Despite the number of other bar opinions approving the use of SaaS products for case or practice, document, and billing/financial management, or storage of client files, billing information, and work product, on remote servers, the North Carolina Bar felt compelled to specifically ask and then answer this question

in the affirmative, “provided steps are taken to minimize the risk of inadvertent or unauthorized disclosure of confidential client information and to protect client property, including the information in a client’s file, from risk of loss." The opinion includes a list of points lawyers should consider when evaluating SaaS vendors in order to minimize potential security risks.

IV. The Lawyer's Duty

All of the opinions make clear that the lawyer's duty is that of competence and reasonable care in selecting and working with any third-party service provider. The opinions also make clear that you are not required to guarantee that the methods of access and storage are infallibly secure and invulnerable to unauthorized access. Just as you cannot guarantee that someone will not break into your office and steal client property. In either circumstance you must take all reasonable steps necessary to minimize the risk of an unauthorized disclosure of client information.

It is your duty to competently investigate and exercise sound professional judgment in forming a reasonable conclusion as to the security of a potential service provider. The following list was compiled from the various state bar ethics opinions and may help in making a reasonable conclusion.

A. Relationship with Service Provider

- Did you perform "due diligence" in checking the background of the service provider?
    - Are they a solid company with a good operating record and a good reputation with others in the field?
    - In what country and state are they located and do business?
- Did you notify the vendor of the confidential nature of the information stored on the firm's servers and in its document database?
- Does the vendor understand a lawyer's professional responsibilities?
- Did you examine the vendor's existing policies and procedures with respect to the handling of confidential information?

B. Create an Enforceable End-Users Licensing Agreement (EULA)

- What is the cost of the service, how is it paid, and what happens in the event of non-payment?
    - Do you loose access to your data, does it become the property of the service provider, or is the data destroyed?
- Are any proprietary rights over your data granted to the service provider?
- Does the vendor assure that confidential client information on your

computer system will be accessed only for technical support purposes and only on an “as needed” basis?

- Does the vendor assure that the confidentiality of all client information will be respected and preserved by the vendor and its employees?
- Do you and the vendor agree on additional procedures for protecting any particularly sensitive client information?
- How is the relationship terminated?
    - What type of notice is required?
    - How do you retrieve your data, is the policy different then that for non-payment ?
- Are there any choice of law or forum, or limitation of damages provisions?

C. Understand the Security Measures

- Know how these things work
    - Encryption
        - Is there an encrypted connection to which to send your information?
        - Will you have the ability to encrypt some data using higher level encryption tools?
        - Was the service provider’s initial encryption scheme tested by an independent auditor?
    - Secure Socket Layer (SSL) - This an industry standard that ensures that the communications between your computers and the cloud-based server are encrypted and protected from interception
    - Intrusion detection - What security measures are used to protect the servers and keep out hackers?
    - Firewalls
    - Passwords - Who has access to the passwords?
    - Tiered data center - The Uptime Institute's tiered classification system is an industry standard approach to site infrastructure functionality. Tier 4 data centers have the most stringent protection for their servers.
    - Does the company conduct regular security audits, in-house or third-party?

D. What Happens to the Data Itself

- Retrieving the data
    - What if the service provider goes out of business, or there is a break in continuity (sales, merger, etc.)
    - Server failure
    - You close your account/cancel the service
        - Will you be able to take the data with you.
        - Make sure data will be returned in a readable format.
- Back-up policies;
    - How often is data backed-up, and are backups distributed across

geographic regions? Backups should not be located in only one place, in case something catastrophic happens at that location.
    - What are the steps to recover data?
- Are you able to quickly sort, organize, search, and produce your data
- Where are the servers located? It should not be located outside the U.S. where it might be subject to foreign laws. Foreign privacy laws can differ markedly from U.S. law
- Who has access to your data? Can employees of the service provider access the stored data, and is their access restricted and tracked? Do the service provider's employees understand their responsibilities regarding confidentiality?
- What would the service provider do if served with a subpoena? Federal laws like the Gramm-Leach-Bliley Act (financial services modernization) and the Health Information Portability and Accountability Act (HIPPA) require safeguards to be in place to prevent disclosure of private and personal information. How does the service provider meet these federal requirements?
- Will you have unrestricted access to the stored data? Is your data stored elsewhere so that if access is thwarted you can acquire the data via another source?

E. Security Begins in the Office

- Client security includes the security of the desktop or laptop from which you are accessing the service.
- All office computers need to be properly secured with firewall and anti-virus protection, and the latest security updates for your operating system and web browsers.
- Enforce strict password protocols; use a password generator.
- Employees have to be trained to use the products and everyone held to the same security standards.

V. Conclusion

The primary and final responsibility for file integrity, maintenance, disposition, and confidentiality rests with you. Addressing the issues above should help you find the best cloud computing service provider for your practice, while also ensuring that your law firm is taking the necessary steps to minimize the risk of inadvertent disclosure of confidential client information. And finally, recognizing your limitations is also part of exercising professional competence. If

you have neither the time nor the inclination to develop sufficient technical knowledgeable then hire a consultant.