Come Rain or Shine: Understanding the Risks and Benefits of Cloud Computing

Michelle J. Weil
Charleston School of Law
Upper Level Writing (5,122 words)
April 20, 2012

The legal profession highly regards precedent and typically mistrusts change.[1] Most attorneys lag behind when it comes to adopting emerging Internet-technologies, such as cloud computing. Nevertheless, in our ever-changing, high-tech society, attorneys cannot afford to ignore current technological advances and modern trends.

Many in the legal profession are regarded as "laggards," because they are typically reluctant or slow to learn about, accept, and use emerging technologies.[2] A recent study discovered, excluding Europe, the United States surprisingly lags behind the rest of the world in adopting cloud computing, even though many of the companies driving it are based in the United States.[3] This slower adoption rate reflects general concerns with storing sensitive data in the cloud.[4] The study confirmed that overcoming the fear of security risks is the key to adopting and benefiting from cloud-applications.[5]

In contrast, "early adopters" are a minority group that is usually the first to try new ideas, processes, and services.[6] Ethical obligations may arise when lawyers become early adopters of new technology. Those opposed to cloud computing argue that attorneys should let other businesses resolve any problems with it, instead of possibly putting confidential client data at risk. Nevertheless, it remains true that lawyers have shared client information with third parties for years.[7] In this era of rapidly developing technology, "lawyers now use outside agencies for numerous functions such as

---

[1] CAROLYN ELEFANT & NICOLE BLACK, SOCIAL MEDIA FOR LAWYERS: THE NEXT FRONTIER 188 (2010).
[2] *See Laggards*, BUSINESSDICTIONARY.COM, http://www.businessdictionary.com/definition/laggards.html (last visited Apr. 19, 2012).
[3] Joe McKendrick, *US Lags Much of World in Cloud Computing Adoption: Study*, FORBES, Mar. 29, 2012, *available at* http://www.forbes.com/sites/joemckendrick/2012/03/29/us-lags-much-of-world-in-cloud-computing-adoption-study/.
[4] *See id.*
[5] *Id.*
[6] *Early* Adopters, BUSINESSDICTIONARY.COM, http://www.businessdictionary.com/definition/early-adopters.html (last visited Apr. 19, 2012).
[7] *See* ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 398 (1995).

accounting, data processing and storage, printing, photocopying, computer servicing, and paper disposal."[8] Data stored in the cloud is at least as safe and secure, if not more so, than data stored locally.[9] While attorneys should not necessarily be first to adopt cloud computing, those who do must stay current with the technology.

Even though laggards are still adverse to the concept of cloud computing, many are inadvertently already using it in one form or another.[10] For example, lawyers are conducting online legal research in the cloud if they are using Westlaw, LexisNexis, CaseFinder, or Fastcase. They are most likely exchanging e-mails with a client who uses Gmail, Yahoo, or Hotmail. They may be using document creation or collaboration tools, such as Google Docs, or backup data services, like Mozy, i365, IBackup, Steel Mountain, and Carbonite. Many lawyers are also using social media sites, such as Facebook, Twitter, and LinkedIn. All of these are Web-based services operate in the cloud.[11]

Though some attorneys are not using cloud computing in their practices right now, it is very likely that they will choose to do so within the next few years; therefore, they need to be aware of both the benefits and risks of the technology. So what exactly is cloud computing then?

I. Cloud Computing Defined

"Cloud computing" is a practical innovation that combines several already available technologies and existing concepts into something new and compelling.[12] Cloud computing gets its name from flow charts used to diagram networked computing,

---

[8] *Id.*
[9] James M. McCauley, *Cloud Computing – A Silver Lining or Ethical Thunderstorm for Lawyers?*, 59 VA. L. 49, 51, *available at* http://www.vsb.org/docs/valawyermagazine/vl0211_consultus.pdf.
[10] *See id.*
[11] *Id.* at 49.
[12] GREGOR PETRI, SHEDDING LIGHT ON CLOUD COMPUTING 11 (2010).

wherein a cloud is used to represent the Internet.[13] The popular phrase is merely shorthand for applications that were developed to run on the Internet, or "cloud."[14] Perhaps the best way to describe cloud computing is that it is a "fancy way of saying stuff's not on your computer."[15]

Cloud applications use massive, powerful servers as hosts, and the servers can be accessed by anyone with a suitable Internet connection.[16] By using the Internet to obtain data or run applications, users can access the cloud from virtually anywhere, on any device connected to the cloud. Unlike traditional methods that retain data on a computer or server at a law office or other place of business, data stored in the cloud is kept on large servers somewhere else and supported by a vendor.[17] One CEO of a cloud computing-provider said, "[a]s a customer, you don't know where the resources are, and for the most part, you don't care. What's really important is the capability to access your application anywhere, move it freely and easily, and inexpensively add resources."[18]

Cloud computing is composed of three different service models: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).[19]

---

[13] NICOLE BLACK, CLOUD COMPUTING FOR LAWYERS 2 (2011).
[14] *Id.* at 14.
[15] Quinn Norton, *Byte Rights: Every Silver Lining Has Its Cloud*, MAXIMUM PC, September 2010, *available at* http://dl.maximumpc.com/Archives/MPC0910-web.pdf.
[16] PETRI, *supra* note 9, at 15.
[17] Richard Acello, *Get Your Head in the Cloud,* A.B.A.J., April 2010, *available at* http://www.abajournal.com/magazine/article/get_your_head_in_the_cloud/.
[18] J. Nicholas Hoover, *Interop: Oracle Predicts Cloud Confusion to Continue*, INFO.WK., (Sept. 17, 2008, 3:35 PM), http://www.informationweek.com/news/services/hosted_apps/210602225.
[19] PETRI, *supra* note 9, at 15.

A. SaaS

SaaS provides cloud-based software to consumers.[20] Lawyers who are already using cloud computing are probably primarily using SaaS. Rather than purchasing and installing software to a firm's computer or server, SaaS is simply accessed via a web browser, such as Internet Explorer, Safari, or FireFox.[21] Data is stored in the cloud-provider's data center rather than on a firm's computers. SaaS users simply pay a monthly subscription fee, and upgrades and updates are rolled out continuously.[22]

SaaS includes a variety of services, such as law practice management applications that can help lawyers with conflicts checking, document management and storage, trust account management, timekeeping, and billing.[23] Personal productivity cloud services, such as Google Apps and E-mail also popular because they enable users to easily access programs from their own personal electronic devices.[24] A good example of SaaS is Clio, a completely web-based practice management system that is specifically designed for solo practitioners and small law firms.[25] Important client data is securely accessible from any device, including an iPhone.[26] Credenza is an example of somewhat of a "hybrid." It turns Microsoft Outlook into a professional practice management tool by storing data in the cloud, while mirroring the data locally, which enables attorneys to work offline.[27]

---

[20] ABA Legal Tech. Resource Ctr., *FYI: Software as a Service (SaaS) for Lawyers*, http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/saas.html (last visited Apr. 19, 2012).
[21] *Id.*
[22] *Id.*
[23] Letter from ABA Comm'n on Ethics 20/20 Working Grp. on the Implications of New Tech., to ABA Entities, Cts., Bar Ass'ns, L. Sch., Individuals, and Entities (Sept. 20, 2010) (*available at* http://www.infolawgroup.com/uploads/file/letterhead-client-confidentiality-issues-paper-final-9_20_10-1(1).pdf).
[24] PETRI, *supra* note 9, at 27.
[25] *See e.g.*, CLIO, http://www.goclio.com/ (last visited Apr. 19, 2012).
[26] *Id.*
[27] *See e.g.*, CREDENZA, http://www.credenzasoft.com/ (last visited Apr. 19, 2012).

It can organize calendars, contacts, tasks, notes, documents, phone calls, billable time, expenses, research, and other client information all within Outlook.

B. PaaS

PaaS is an outgrowth of SaaS that allows users to rent hardware, operating systems, storage, and network capacity over the Internet.[28] With PaaS, operating system features can be improved and upgraded frequently.[29] Salesforce.com, a company best known for its Customer Relationship Management (CRM) product, provides a good example of PaaS.[30] The company's platform allows external developers to create add-on applications that integrate into the main application and are hosted on the company's infrastructure.[31]

C. IaaS

IaaS, the most basic cloud service model, provides access to cloud-based, or "virtual" hardware.[32] With IaaS, users can access additional storage or processing capacity over the Internet instead of installing new hardware in the office.[33] The data is stored on servers in the cloud and available on demand by the user. The service provider who owns the equipment is typically responsible for housing, running, and maintaining it.[34] The provider is also responsible for offering technical expertise to manage and support the equipment.[35] Amazon EC2 and Rackspace are examples of this type of service,

---

[28] *Platform as a Service (Paas)*, WHATIS.COM, http://searchcloudcomputing.techtarget.com/definition/Platform-as-a-Service-PaaS (last visited Apr. 19, 2012).
[29] *Id.*
[30] *See e.g., Salesforce.com*, WIKIPEDIA, http://en.wikipedia.org/wiki/Salesforce.com (last visited Apr. 19, 2012).
[31] *Id.*
[32] BLACK, *supra* note 10, at 4.
[33] PETRI, *supra* note 9, at 20.
[34] Nick Pournader, *Embracing Technology's "Cloud" Frontier*, L. PRAC.TODAY, Oct. 2010, *available at* http://apps.americanbar.org/lpm/lpt/articles/pdf/ftr10106.pdf.
[35] *Id.*

which allows users to quickly scale capacity up and down as computing requirements change.[36]

II. Every Cloud Has a Silver Lining: Benefits of Cloud Computing

Cloud computing offers many benefits and is important to the legal profession for a number of reasons. While certainly not an exhaustive list, some possible advantages include expanded storage data, immediate application updates, greater flexibility, and reduced costs.[37]

A. Efficiency

A new law firm can usually be up and running significantly faster with cloud services than if it has to plan, buy, build, and implement in office.[38] Planning time is considerably less since there are fewer logistical issues, and there are no power requirements or space considerations to think about.[39] With many SaaS applications or other cloud offerings operators can start using the service within hours or days rather than weeks or months.[40] Cloud computing also supports automated backups and easy synchronization.[41] Only one application has to be updated, rather than thousands, and updates can be done instantly. As quickly as a new feature is completed, it can be updated on the SaaS platform.[42] Additionally, cloud computing enables attorneys to increase overall efficiency by

---

[36] *See e.g.*, AMAZON WEB SERVICES, http://aws.amazon.com/ec2/ (last visited Apr. 19, 2012); RACKSPACE, http://www.rackspace.com (last visited Apr. 19, 2012).
[37] Nathan Crystal, *Ethics Watch: Technology and Confidentiality, Part Two*, 23 S.C. LAW. 8, Nov. 2011.
[38] BENEFITS OF CLOUD COMPUTING FOR SMALL BUSINESS, http://www.thesmallbusiness.org/software/benefits-of-cloud-computing.html (last visited Apr. 19, 2012).
[39] *Id.*
[40] *Id.*
[41] Richard S. Grant, *Statement before the Ethics 20/20 Comm'n*, http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/ethics_20_20_comments/granat_2011_atlanta_publichearing.authcheckdam.pdf (last visited Ap. 19, 2012).
[42] *Id.*

"outsourcing" tasks such as hosting electronic discovery, timekeeping, case management, and billing.[43]

B. Convenience and Flexibility

Because applications and services are offered over the Internet, users are not limited to using cloud-software or services just at work or only on one computer. Moving to the cloud provides attorneys mobility, offering access to any tools and client data via the Internet anywhere at anytime.[44] Cloud computing enables attorneys to work easily from home, the office, or even on a visit to a client's home.[45]

Most cloud services are also platform independent.[46] Web-based software is not designed specifically for any one browser or operating system, making it is possible for individuals with Windows, Mac, and Linux operating systems to use the same applications.[47] Most applications can be accessed through tablets and mobile phones, eliminating the need for multiple versions of software for the same program.[48]

C. Reduced Costs

With cloud computing, resources are shared, as well as the costs. Cloud computing reduces operational costs by allowing lawyers to cheaply store and access data and software programs in the cloud.[49] Both large and small law firms can save money, as the cost of owing and maintaining data centers, servers, and computer software can be excessive for many law firms. Firms utilizing SaaS do not have to purchase servers and

---

[43] Jason Gonzalez & Linn Freedman, *Mobile Devices and Attorney Ethics: What are the Issues?*, ABA/BNA LAW. MANUAL ON PROF'L CONDUCT, Vol. 27, No. 26. 792, 794 (2011).
[44] Grant, *supra* note 37.
[45] *Id.*
[46] BENEFITS OF CLOUD COMPUTING FOR SMALL BUSINESS, *supra* note 34.
[47] *Id.*
[48] *Id.*
[49] Nicole Black, *3 Things Lawyers Should Know about Cloud Computing*, SMALL FIRM INNOVATION (July 8, 2011), http://www.smallfirminnovation.com/2011/07/3-things-lawyers-should-know-about-cloud-computing/.

software, pay expensive software licensing and upgrade fees, or hire IT staff; the cloud provider eliminates all of this for a simple monthly fee.[50] The monthly cost is usually based on the number of users, sometimes with tiered pricing.[51]

III. A Little Rain Must Fall: Risks of Cloud Computing

Cloud-computing companies were not created with lawyers' ethical obligations to keep client data safe and secure in mind. Thus, the idea of cloud computing causes security and privacy concerns for many lawyers. A solution to these concerns is for a lawyer considering cloud computing to have sufficient knowledge to make an informed decision that a potential cloud-computing vendor is employing "best practices" to store information in a manner compatible with the lawyer's ethical obligations.[52]

A. Security

Although cloud computing poses some possible security risks, lawyers should use the same standards that apply to physical client files when using cloud computing.[53] Attorneys are obligated to ensure that confidential client data is secure, whether they store paper documents in a warehouse or outsource to a third-party provider. When client information is stored in a warehouse or on an in-house server, many lawyers feel that it is better protected. Attorneys also need their clients to feel secure that their confidential information will be safeguarded.

Unfortunately, many lawyers place their client's confidential data at risk on a regular basis and do not even know it.[54] There are statistics that show that one-third of security

---

[50] BLACK, *supra* note 10, at 20.
[51] ABA Legal Tech. Resource Ctr., *supra* note 17.
[52] Grant, *supra* note 37.
[53] BLACK, *supra* note 10, at 27.
[54] *See* Elinor Mills, *Cloud Computing Security Forecast: Clear Skies*, CNET (Jan. 27, 2009 4:00 AM), http://news.cnet.com/8301-1009_3-10150569-83.html.

breaches result from stolen or lost laptops and other devices.[55] Risk can also occur when lawyers simply communicate with their clients over e-mail.[56] Still, most ethics committees have concluded that using e-mail to communicate with clients does not constitute an ethical violation.[57] According to an ABA Formal Opinion, a lawyer who is sending or receiving communications with a client via e-mail must warn the client about the risk of sending or receiving e-mails where there is a significant risk that a third party may gain access.[58] Further, a law firm that suffers a substantial security breach is ethically required to inform its clients about the breach, so the clients can make informed decisions about the problem.[59] It is recommended for law firms to include provisions dealing with the use of technology is their engagement agreements.[60] When storing data in the cloud, there is a potential for security breaches, but many cloud computing vendors incorporate some form of encrypted client communication into their platforms, thereby reducing the inherent security flaw in most e-mails.[61]

The technology and expertise of cloud-providers is usually greater than that at most law firms. While vendors have elaborate and redundant security and backup systems to ensure data is protected from accidental loss and unauthorized access, firms that fail to back up their data off-site unnecessarily risk losing their data in face of a break in or natural disaster.[62] "Cloud computing can be as secure, if not more secure, than the

---

[55] *Id.*
[56] *See, e.g.*, ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 413 (1999) (discussing the confidentiality of unencrypted e-mail).
[57] *Id.*
[58] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 459 (2011) (discussing duty to protect the confidentiality of e-mail communications with one's client).
[59] Crystal, *supra* note 33.
[60] *Id.*
[61] BLACK, *supra* note 10, at 24.
[62] *Id.* at 25.

traditional environment," said Eran Feigenbaum, director of security for Google Apps.[63] According to Peter Coffee, director of platform research at Salesforce.com, cloud service providers are held to high standards. They must offer evidence of security certifications, and are subject to inspections by auditors, placing them under much higher scrutiny than typical in-house security teams.[64] Many lawyers are so busy that they do not have the time to maintain their computer systems, and many do not understand the importance of updating software in order to install new security patches.[65] Thus, if in-house security capabilities are not sufficient, cloud computing could actually increase overall security.[66]

Computer hacking poses special problems for law firms. One popular hacker strategy is to hack small, minimally secured sites.[67] Mandiant, a company that specializes in detecting and responding to security breaches, said it estimates that around eighty major United States law firms were hacked in 2011.[68] The level of skill and seriousness of the attacks differed widely, but law firms representing celebrities, for example, were top targets, according to a researcher at a cyber security firm.[69] Most recently, a Virginia-based law firm was hacked because its Google e-mail passwords were not secure enough

[63] Mills, *supra* note 48.
[64] *Id.*
[65] BLACK, *supra* note 10, at 29.
[66] Gonzalez & Freedman, *supra* note 39, at 794.
[67] *See The Top 10 Hacker-Defense Strategies for Small Business*, WALL ST. J., July 21, 2011, *available at* http://www.wipfli.com/resources/images/23516.pdf.
[68] Michael A. Riley & Sophia Pearson, *China-Based Hackers Target Law Firms to Get Secret Deal Data*, BLOOMBERG (Jan. 31, 2012, 4:37 PM), http://www.bloomberg.com/news/2012-01-31/china-based-hackers-target-law-firms.html.
[69] *Id.*

to keep out hackers.[70] Security experts recommend hiring an outside auditor at least annually who is capable of checking for security lapses and fixing any holes.[71]

"Absolute security" is not a possibility; even if attorneys are not utilizing cloud services, third parties can still gain access to client information.[72] Ethics committees, acknowledging absolute security is not feasible, do not require lawyers to lockdown their documents, but only to use reasonable measures to keep them safe.[73]

B. Privacy

Whether privacy concerns prevent a firm from using cloud computing depends primarily on the area of practice. Lawyers might be obligated to comply with certain privacy laws and regulations. For example, firms that handle client data subject to either the Health Care Portability and Accountability Act (HIPAA) or the Gramm-Leach-Bliley Act must comply with specific regulations before disclosing client data to a third party, including a cloud-computing provider.[74] The Health Information Technology for Economic and Clinical Health Act (HITECH Act) that went into effect in February 2010 extends the confidentiality requirements of HIPAA.[75] According to the notification requirements set forth by the HITECH Act, any security breaches, including those that occur on the could provider's end, must be immediately reported.[76] The Act imposes

---

[70] Martha Nell, *Unaware 'Anonymous' Existed Until Friday, Partner of Hacked Law Firm is Now Fielding FBI Phone Calls*, A.B.A.J. (Feb. 6, 2012, 3:02 PM), http://www.abajournal.com/news/article/unaware_that_anonymous_hacking_group_existed_until_friday_law_firm_partner/.

[71] Jason Krause, *Hack Attack*, A.B.A.J., Nov. 2002, 51, 53, *available at* http://books.google.com/books?id=YawKzp-oo_cC&pg=PT53&lpg=PT53&dq=aba+law+firms+hacked&source=bl&ots=Q9P4wWq8lZ&sig=3ReqwVXVKHLwZCcpNkHlcoBdNTM&hl=en&sa=X&ei=rOdoT8i5KanMsQKE7rSTCQ&ved=0CEkQ6AEwBg#v=onepage&q=aba%20law%20firms%20hacked&f=false.

[72] Black, *supra* note 43.

[73] *Id.*

[74] BLACK, *supra* note 10, at 80.

[75] *Id.*

[76] *Id.*

harsh penalties of up to $50,000 per violation if a law firm fails to comply with the requirements.[77] Forty-six states, the District of Columbia, Puerto Rico, and the Virgin Islands have enacted security breach notification laws that typically require parties in control of electronically stored personal information to notify any individuals affected by a data breach.[78] Thus, these laws would require notification if any personal client information stored in the cloud is inadvertently disclosed.

A client's data stored in the cloud may also be subject to discovery and must be easily accessible if requested during litigation.[79] A lawyer must be careful not to enter a contract of adhesion with a cloud-provider where he or she does not have any control over the data stored in the cloud.[80] The lawyer must be diligent in seeking out a company that disavows any authority to access a customer's data in its terms of service agreement.[81] The agreement with the cloud-provider should clearly state that the data belongs to the law firm. For example, Remember the Milk is a cloud-provider that disavows any authority to access a customer's data in its terms of service agreement.[82] Likewise, Mozy's terms of service agreement provides that it "will not view the files that you backup using the Service."[83] It is also important for a lawyer to confirm that all data will stay within the United States.

---

[77] *Id.*
[78] *See State Security Breach Notification Laws*, NAT'L CONFERENCE OF STATE LEGISLATION (Feb. 6, 2012), http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx.
[79] McCauley, *supra* note 7, at 52.
[80] *See Cloud Computing Agreements Should Not Be Cloudy*, HG.ORG (Oct. 12, 2010), http://www.hg.org/article.asp?id=20072.
[81] *Id.*
[82] *See e.g.,* REMEMBER THE MILK, *Intellectual Property Rights*, http://www.rememberthemilk.com/help/terms.rtm (last visited Apr. 19, 2011) ("We will not use any of your content for any purpose except to provide you with the Service.").
[83] MOZY, *Decho Corporation Privacy Policy*, http://mozy.com/privacy (last visited Apr. 19, 2011).

IV. Head in the Cloud: Ethical Obligations

Many lawyers are lagging behind when it comes to cloud computing because they have ethical reservations. While the Model Rules of Professional Conduct do not expressly require lawyers to stay current with the latest technological advances, several provisions appear to imply a duty to monitor such developments and to understand the potential benefits and risks of new communication technology.[84] While the ABA has not yet issued a formal opinion, several state bar associations are publishing new opinions about cloud computing and third-party providers. The opinions that have addressed cloud computing consider it to be acceptable, so long as attorneys adequately consider and address the risks.[85] But, they also require attorneys to engage in a level of scrutiny of the cloud providers that is most likely unfamiliar to many lawyers.[86]

A. Duty of Competence

The duty of competence, set forth in Model Rule 1.1, provides that a lawyer must have "the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation" of a client.[87] Many bar associations have interpreted this rule to also include knowledge of the security issues involved in attorneys' use of technology.[88] The State Bar of Arizona opined,

> an 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

[84] Roland L. Trope & Sarah Jane Hughes, *Contemporary Issues in Cyberlaw: Red Skies in the Morning – Professional Ethics at the Dawn of Cloud Computing*, 38 WM. MITCHELL L. REV. 111, 137 (2011).
[85] Gonzalez & Freedman, *supra* note 39, at 794.
[86] Crystal, *supra* note 33.
[87] MODEL RULES OF PROF'L CONDUCT R. 1.1 (2008).
[88] Gonzalez & Freedman, *supra* note 39, at 792.

> obtain that competence is ethically required to retain an expert consultant who does have such competence.[89]

Attorneys will likely be held responsible for keeping reasonably informed about rapidly developing technology and security risks; just being aware of current technological security issues is not enough.[90] They are expected to "stay current with the technological advances" to ensure that the provider's security procedures are adequate.[91] The duty of competence extends not only to attorneys, but also to the supervision of non-attorney staff.[92] They too must make reasonable efforts to use technology in a secure manner. Moreover, lawyers must recognize the risks inherent with new communications and advise their clients accordingly.[93]

The Oregon State Bar answered with "[y]es, qualified," in response to whether a law firm may contract with a third-party vendor to store client files and documents online on a remote server, so that the lawyer and client could access the documents over the Internet from any location.[94]

> A [l]awyer may store client materials on a third-party server so long as [the] [l]awyer complies with the duties of competence and confidentiality to reasonably keep the client's information secure within a given situation. To do so, 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 though a third-party vendor's compliance with industry standards relating to confidentiality and security, provided that those industry standards meet the minimum

---

[89] Ariz. State Bar Ass'n Standing on Comm. on Ethics and Prof'l Responsibility, Formal Op. 05-04 (July 2005), *available at* http://www.myazbar.org/Ethics/opinionview.cfm?id=523.
[90] Gonzalez & Freedman, *supra* note 39, at 793.
[91] N.Y. State Bar Ass'n Standing on Comm. on Ethics and Prof'l Responsibility, Formal Op. 842 (Sept. 2010), *available at* http://www.infolawgroup.com/uploads/file/http___www_nysba_org_AM_Template_cfm_Section=Ethics_Opinions&TEMPLATE=_CM_ContentDisplay.pdf.
[92] *Id.*
[93] Trope & Hughes, *supra* note 74, at 138.
[94] Or. State Bar Ass'n Standing on Comm. on Ethics and Prof'l Responsibility, Formal Op. 188 (2011), *available at* http://www.osbar.org/_docs/ethics/2011-188.pdf.

> requirements imposed on the [l]awyer by the Oregon RPCs. 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 that vendor notify Lawyer of any nonauthorized third-party access to the materials. Lawyer should also investigate how the vendor backs up and stores its data and metadata to ensure compliance with the Lawyer's duties.[95]

The opinion further stated that, as technology advances, a lawyer might be required to reevaluate the protective measures used by the third-party vendor to safeguard the client materials.[96]

B. Duty of Due Diligence

Model Rule 1.3 requires lawyers to act with "reasonable diligence and promptness in representing a client."[97] The Rules objectively measure reasonableness,[98] and there is nothing in them that appears to prohibit a move to the cloud when appropriate due diligence is performed. In order for a lawyer to claim that he or she has taken reasonable precautions, the lawyer must do his or her due diligence in researching and understanding the risks and benefits of cloud-technology.[99] Attorneys who use cloud computing should develop due diligence strategies and procedures, document them, and more importantly, follow them, even though the process may turn out to be very time consuming.

The North Carolina Bar published a formal ethics opinion in 2011, regarding an attorney's due diligence when selecting a cloud provider.

> [A] law firm may use SaaS if reasonable care is taken to minimize the risks of inadvertent disclosure of confidential information and to protect the security of client information and client files. A lawyer must fulfill the duties to protect confidential client information and to safeguard client files by applying the same diligence and

[95] *Id.*
[96] *Id.*
[97] MODEL RULES OF PROF'L CONDUCT R. 1.3 (2008).
[98] *See id.* at R. 1.0(h) (Terminology).
[99] BLACK, *supra* note 10, at 37.

> competency to manage the risks of SaaS that the lawyer is required to apply when representing clients.[100]

Recognizing that technology and security risks change so rapidly, the opinion does not list any specific minimum requirements a lawyer must follow in selecting a SaaS-provider because such requirements might quickly become outdated.[101] Instead, it provides five "recommended" security measures, which include checking for confidentiality provisions in the vendor's user agreement, assessing the ability to retrieve any data, reviewing security policies, evaluating how the vendor stores and secures data, and reviewing how the vendor backs up the data.[102] In considering these issues, lawyers may want to consult with "professionals competent in the area of online security."[103]

Similarly, Iowa lawyers may use any form of SaaS to store client information and other data in the cloud, so long as they have "unfettered access to the data" and can reasonably verify that sound methods are being used to protect the information.[104] The Iowa State Bar's Ethics Committee said it believes that Iowa Rules of Professional Conduct establish a "reasonable and flexible approach" to cope with "ever-changing technology."[105] Lawyers must exercise due diligence to assess the security and reliability of the cloud provider and act accordingly.[106] This committee recognized that preforming due diligence concerning information technology can be complex. Due diligence must be performed by individuals who posses the both the technical expertize and a thorough

---

[100] N.C. State Bar Ass'n Standing on Comm. on Ethics and Prof'l Responsibility, Formal Op. 6 (Jan. 2011), *available at* http://www.ncbar.gov/ethics/ethics.asp?page=484.
[101] *Id.*
[102] *Id.*
[103] *Id.*
[104] Letter from Iowa State Bar Ass'n Comm. On Ethics and Practice Guidelines, to Dwight Dinkla, Executive Director, Iowa State Bar Ass'n (Sept. 9, 2011) (*available at* http://www.iabar.net/ethics.nsf/e61beed77a215f6686256497004ce492/02566cb52c2192e28625791f00834cdb/$FILE/Ethics%20Opinion%2011-01%20--%20Software%20as%20a%20Service%20-%20Cloud%20Computing.pdf).
[105] *Id.*
[106] *Id.*

understanding of the Iowa Rules of Professional Conduct. Hence, a lawyer may rely on the due diligence of services of independent companies, bar associations, or other similar organizations.[107]

The Pennsylvania Bar Association Committee on Legal Ethics and Professional Responsibility concluded that an attorney may store confidential client information in the cloud, but it recognized that most service agreements are presented on a "take it or leave it" basis. Because the need to maintain confidentiality is crucial to the attorney-client relationship, attorneys have a professional obligation to facilitate an agreement that adequately safeguards security and reliability.[108] Unlike other states' ethics opinions relating to cloud computing, the Pennsylvania opinion lists suggestions for establishing the standard of reasonable care. According to the opinion, lawyers generally should implement internal mechanisms to:

- Back up data;
- Install firewalls;
- Limit access of information to others;
- Avoid inadvertent disclosure of information;
- Encrypt confidential data;
- Implement electronic audit trail procedures to monitor who is accessing data; and
- Craft plans to address security breaches.[109]

When choosing a cloud provider, lawyers should investigate the provider's security measures, backup systems, and disaster safeguards, ensuring the provider:

- Explicitly agrees that it has no ownership interest in the data;
- Has an obligation to preserve the data;
- Will alert the lawyer if a third-party requests information;
- Uses technology designed to withstand cyber attacks;
- Describes in its service agreement how confidential client information will be handled;

[107] *Id.*
[108] Pa. Bar Ass'n Comm. on Legal Ethics & Prof'l Responsibility, Formal Op. 2011-200 (2011), *available at* http://op.bna.com/mopc.nsf/id/kswn-8pcm4u/$File/2011-200.pdf.
[109] *Id.*

- Allows the lawyer to audit the provider's security procedures;
- Will host the firm's data only within the United States;
- Provides a method for retrieving data if the lawyer terminates use or the vendor goes out of business; and
- Allows the lawyer to get data "off" the vendor's servers.[110]

In order to ensure a third-party vendor's security procedures are always adequate, attorneys must "stay current with technological advances."[111]

C. Duty of Confidentiality

Attorneys are not required to guarantee that a breach of confidentiality will not occur when using an outside service provider, but the Rules do require that lawyers act with reasonable care to protect client information. Model Rule 1.6(a) provides that an attorney generally may "not reveal information relating to the representation of a client" without the client's informed consent.[112] The comments further provide that a lawyer must "act competently" to avoid any unauthorized disclosure of client information and "must take reasonable precautions to prevent the information from coming into the hands of unintended recipients."[113]

An attorney's obligation to preserve confidential client information extends beyond merely prohibiting an attorney from revealing information without a client's consent.[114] A lawyer must take reasonable care to affirmatively protect a client's confidential data, whether reduced to digital format, paper, or otherwise.[115] The New York Committee on Professional Ethics determined that attorneys are permitted to use an online cloud computer data backup system to store client information if they take reasonable

---

[110] *Id.*
[111] N.Y. Formal Op. 842, *supra* note 81.
[112] MODEL RULES OF PROF'L CONDUCT R. 1.6 (2008).
[113] *Id.* at cmt. 16, 17.
[114] N.Y. Formal Op. 842, *supra* note 81.
[115] *Id.*

precautions, such as ensuring that the provider has an obligation to preserve confidentiality and uses available technology to guard against hackers.[116]

> Because the inquiring lawyer will use the online data storage system for the purpose of persevering client information – a purpose both related to the retention and necessary to providing legal services to the client – using the online system is consistent with conduct that this Committee has deemed ethically permissible.[117]

Exercising "reasonable care," however, does not require that the lawyer guarantees client information is secure from any unauthorized access.[118] Likewise, Nevada's Ethics Committee analogized storing digital files on a third party's off-site server to storing paper documents in a third party's off-site storage facility. So long as a lawyer exercises reasonable care in selecting the vendor and has a reasonable expectation that the vendor will keep the data confidential and inaccessible by others the requirements of Rule 1.6 are met.[119] Ultimately, common sense should prevail.

D. Duty to Safeguard Client Property

Model Rule 1.15 requires a lawyer to safeguard client property for a period of five years after termination of representation.[120] Lawyers who use cloud computing must confirm the provider has a return and retention policy that ensures there are methods in place to remove data and return it to a client.[121] In regards to Rules 1.6 and 1.15 some state bars are concerned that a lawyer may not have the technical knowledge to select an appropriate provider.[122] As a remedy, several proposed state bar ethics opinions that

---

[116] *Id.*
[117] *Id.*
[118] *Id.*
[119] Nev. State Bar Ass'n Standing on Comm. on Ethics and Prof'l Responsibility, Formal Op. 33 (2006), *available at* http://ftp.documation.com/references/ABA10a/PDfs/3_12.pdf.
[120] MODEL RULES OF PROF'L CONDUCT R. 1.15 (2008).
[121] BLACK, *supra* note 10, at 43.
[122] *Id.* at 37.

approve cloud computing require attorneys to consider several security-related questions, such as:

- Where will the data physically be located? Will the attorney have unrestricted access to the data? Does the attorney have another copy of the data if the vendor limits access for any reason?
- What is the company's reputation? Has the company ever experienced any security breaches? If so, how were they handled? Where is the company situated?
- What does the vendor agreement provide regarding who "owns" the data? Will the data be destroyed if the relationship terminates? If so, will the vendor provide written confirmation that is was destroyed?
- What security measures does the vendor use? Are passwords used? Is encryption used?
- What does the vendor do to ensure its employees are trustworthy? Can the vendor's employees view the data?
- What are the company's disaster recovery procedures? Does the company keep a backup copy of the data in case of an emergency?
- Will the company notify the attorney if it is served with a discovery request?
- What are the companies notification policies regarding a data breach?[123]

There are not a specific number of "correct" answers for a service to be acceptable, but reasonable efforts must be used to ensure confidential data is kept secure.[124]

V. Forecast: Increasing "Cloudiness"

Cloud computing is not flawless, but over time the security and ethical issues specific to lawyers who handle confidential client information will be resolved.[125] Two organizations with the goal of creating unified standards for legal cloud computing were recently established, The Legal Cloud Computing Association (LCCA) and the International Legal Technologies Standards Organization (ILTSO).[126] ILTSO was formed in early 2011 and its goal is to "promote secure and ethically-conscious

[123] Gonzalez & Freedman, *supra* note 39, at 794.
[124] *Id.*
[125] Black, *supra* note 43.
[126] BLACK, *supra* note 10, at 26.

technology standards for the legal profession."[127] In order to keep the standards current with new changes in technology, the organization intends to update the standards on a regular basis. It hopes to provide state bars with the guidance they may need to safely use cloud computing in the legal field.[128]

The ABA Commission on Ethics 20/20 debated whether to recommend modifying the Model Rules to account for the unique confidentiality concerns that arise when lawyers transmit and store data off-site and drafted a proposal "designed to give lawyers more guidance regarding their confidentiality-related obligations when using technology."[129] The Commission considered three different alternatives, not mutually exclusive. First, the Commission elected to produce White Papers to explain some problems and possible solutions regarding lawyers' use of technology.[130] Second, the Commission suggested that the ABA create a user-friendly, continuously updated website that helps lawyers stay abreast of changes in technology and describes useful practices for dealing with those changes.[131] Ultimately, the Commission proposed amendments to the Model Rules of Professional Conduct, such as Model Rules 1.1 (competency) and 1.6 (duty of confidentiality), or the comments to those Rules.[132] It concluded that the basic principles underlying the current Model Rules are applicable to new developments in technology.[133] Hence, many of the recommendations involve clarification and expansion of existing

---

[127] http://www.iltso.org/iltso/Standards_files/ILTSO%20Master%20Document%202011%20Final.pdf
[128] BLACK, *supra* note 10, at 40.
[129] *2011 Guidelines for Legal Professionals*, INT'L LEGAL TECH. STANDARDS ORG., *available at* http://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/20110502_technology.authcheckdam.pdf.
[130] Letter from Jamie S. Gorelick & Michael Traynor, Co-Chairs ABA Comm'n. on Ethics 20/20, to ABA Entities, Cts., Bar Ass'ns, L. Sch., and Individuals (Dec. 28, 2011) (*available at* http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/20111228_summary_of_ethics_20_20_commission_actions_december_2011_final.authcheckdam.pdf).
[131] *Id.*
[132] *Id.*
[133] *Id.*

Rules in attempt to apply the core values of the legal profession to today's technological challenges.[134] The Commission proposed a new paragraph (c) in Model Rule 1.6 and related amendments to the Comments that would make clear that "[a] lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relation to the representation of a client."[135] Any unauthorized access to or inadvertent disclosure of confidential information would not constitute a violation if the "lawyer has made reasonable efforts to prevent the access or disclosure."[136] An amendment to Comment [16] lists several proposed factors to be considered in determining the reasonableness of the lawyer's efforts, such as the sensitivity of the information, the likelihood of disclosure if the lawyer does not employ additional safeguards, the cost and difficulty of employing additional safeguards, and the extent to which additional safeguards may adversely affect the lawyer's ability to represent clients.[137] The Commission also proposed amendments to Comment [6] of Model Rule 1.1 to emphasize that in order to keep abreast of changes in the practice of law, attorneys should have a basic understanding of the "benefits and risks associated with technology."[138]

To date, not a single ethics panel has found any ethical concerns with lawyers' use of cloud computing provided they exercise reasonable care in selecting a vendor. Regardless of whether lawyers are storing files in the cloud or in their office, they must make a "reasonable effort" to keep client's information secure. As technology advances

---

[134] *Id.*
[135] ABA Comm'n on Ethics 20/20, Revised Draft Resolutions for Comment (Feb 21, 2012) (regarding technology and confidentiality), *available at* http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/20120221_ethics_20_20_revised_draft_resolution_and_report_technology_and_confidentiality_posting_final.authcheckdam.pdf.
[136] *Id.*
[137] *Id.*
[138] *Id.*

and cloud computing becomes more prevalent in the legal field, attorneys still adverse to it will nevertheless have a duty to understand the benefits and risks associated with it, even if only to adequately advise their clients.