The John Marshall Journal of Information Technology & Privacy Law

Volume 31 | Issue 1 Article 4

Fall 2014

The Ethical Implications of Cloud Computing for Lawyers, 31 J. Marshall J. Info. Tech. & Privacy L. 71 (2014)

Stuart Pardau

Blake Edwards

THE ETHICAL IMPLICATIONS OF CLOUD COMPUTING FOR LAWYERS

STUART L. PARDAU & BLAKE EDWARDS*

I. INTRODUCTION

In late 2010 Australian mining and petroleum company BHP Billiton Ltd. ("Billiton") was working on a $38 billion deal for the acquisition of Saskatchewan-based Potash Corp. ("Potash") when hackers launched a cyber-attack against Toronto law firms involved in the transaction, including prominent "Bay Street" firms Blake Cassels & Graydon LLP (representing BHP Billiton) and Stikeman Elliott LLP (representing Royal Bank of Canada).[1] Billiton's acquisition of Potash would have made Billiton the world's foremost producer of potash, and some observers suspected that the Chinese government sponsored the attack to protect the interests of Sinochem Group, China's state-owned chemicals and fertilizer company.[2] The Billiton-Potash deal ultimately fell through, allegedly for other reasons, and the law firms involved insisted that no confidential information was compromised.[3] However, the attack caught the attention of authorities in the United States. The following year, the Federal Bureau of Investigation (FBI) began organizing meetings with top 200 law firms in New York City, and in other

---

* Stuart L. Pardau received his J.D. from Stanford Law School and is currently an Assistant Professor of Business Law at the David Nazarian College of Business and Economics, California State University, Northridge. Blake Edwards received his J.D. from Pepperdine University, where he was editor in chief of the Pepperdine Law Review. After clerking on the United States Court of Appeals for the Fifth Circuit, he worked as a legal reporter at the Daily Journal in Los Angeles and then moved to Egypt.

1. *See* Michael A. Riley & Sophia Pearson, *China Based Hackers Target Law Firms to Get Secret Deal Data*, BLOOMBERG (Jan. 31, 2012, 3:37 PM), http://www.bloomberg.com/news/2012-01-31/china-based-hackers-target-law-firms.html.

2. Jeff Gray, *Hackers linked to China sought Potash deal details: consultant*, THE GLOBE AND MAIL (Nov. 30, 2011, 3:37PM), http://www.theglobeandmail.com/technology/tech-news/hackers-linked-to-china-sought-potash-deal-details-consultant/article534297/ ("Sinochem Group, China's state-owned chemicals and fertilizer group, is thought to have considered its own bid for Potash Corp., out of fear that BHP would control the global supply for potash.").

3. *See* Riley & Pearson, *supra* note 2.

major markets across the country, to discuss cyber security.[4] While banks and large companies had spent preceding years beefing up security measures, law firms were apparently lagging behind, opening themselves up to attacks like those that occurred in Canada. According to Mary Galligan, who was the head of the cyber division in the FBI's New York office at the time, "[a]s financial institutions in New York City and the world become stronger, a hacker can hit a law firm and it's a much, much easier quarry."[5]

But cyber security isn't just a big firm problem. "Cloud computing," which involves the use of third party servers to store data and run software remotely, has become widely available and enormously popular in recent years—contracts, deposition transcripts, financial records, correspondence, and other sensitive information which were once stored in cardboard boxes and file cabinets are now kept online, where, for better or worse, they can be accessed quickly and easily from anywhere.[6] A multi-billion dollar, multi-national acquisition like the Billiton-Potash deal might draw the special attention of sophisticated, state-backed hackers, but, in the event of a broad security breach, solo practitioners and small firms are just as answerable to clients if privileged or confidential information is breached in cyberspace.

In spite of security concerns, lawyers have begun to avail themselves of cloud computing's efficiencies.[7] However, there is still confusion about the ethical implications that surround cloud computing. The lawyer is under strict obligations to offer competent representation, to protect the client's confidences and property, and to ensure that non-lawyers, whom lawyers hire, are abiding by comparable standards. In 2012 the American Bar Association (ABA) suggested in Comment 8, to Model Rule of Professional Responsibility 1.1, that attorneys "keep abreast of . . . the benefits and risks associated with relevant technology."[8] Commentators note that Comment 8 puts lawyers on notice that they can no longer be ignorant about technologies like cloud compu-

---

4. *See id.*; Matthew Goldstein, *Law Firms Are Pressed On Security for Data*, N.Y. TIMES (Mar. 26, 2014, 7:00 PM), http://dealbook.nytimes.com/2014/03/26/law-firms-scrutinized-as-hacking-increases/?_php=true &_type=blogs&_r=0.

5. *See* Riley & Pearson, *supra* note 2.

6. *See, e.g.,* Reuven Cohen, *The Cloud Hits the Mainstream: More than Half of U.S. Businesses Now Use Cloud Computing*, FORBES (Apr. 16, 2013), http://www.forbes.com/sites/reuvencohen/2013/04/16/the-cloud-hits-the-mainstream-more-than-half-of-u-s-businesses-now-use-cloud-computing/.

7. Nicole Black, *Lawyers' Use of Cloud Computing on the Rise in 2012*, MY CASE (Dec. 4, 2012), http://www.mycase.com/blog/2012/12/lawyers-use-of-cloud-computing-on-the-rise-in-2012/.

8. MODEL RULES OF PROF'L CONDUCT R. 1.1 cmt. 8 (2012).

ting.[9] But what, exactly, does that require? Sixteen different state bar associations have made various attempts to help attorneys navigate the issue of cloud computing, but their opinions on cloud computing are generally impractical and blind to the attorney's lack of leverage with vendors.[10] This is unfortunate. In spite of the headline-grabbing cyber-

---

9. Darla Jackson, *Can Lawyers Be Luddites? Adjusting to the Modification of the ABA Model Rules of Professional Conduct Regarding Technology,* 84 OKLA. BAR J. 2637 (2013).

10. *See* Ala. State Bar Ethics Op. 2010-02 (2010), *available at* http://www.alabar.org/ogc/PDF/2010-02.pdf (Attorney can outsource storage of client files if he takes reasonable steps to make sure data is protected); Az. State Bar Ethics Op. 09-04 (2009), *available at* http://www.azbar.org/Ethics/EthicsOpinions/ViewEthicsOpinion?id=704 (Attorney can use online file storage and retrieval system that enables clients to access their files over the Internet, as long as she takes reasonable precautions to protect confidentiality of the information); Cal. State Bar, Formal Op. 2010-179 (2010), *available at* http://ethics.calbar.ca.gov/LinkClick.aspx?fileticket= wmqECiHp7h4%3D&tabid=837; Iowa State Bar Comm. on Ethics, Formal Op. 11-01 (2011), *available at* http://www.iabar.net/ethics.nsf/e61beed77a2 15f6686256497004ce492/02566cb52c2192e28625791f00834cdb/$FILE/Ethics%20Opinion %2011-01%20--%20Software%20as%20a%20Service%20-%20Cloud%20Computing.pdf (Appropriate due diligence a lawyer should perform before storing files electronically with a third party using SaaS (cloud computing), includes determining that attorney will have adequate access to the stored information and will be able to restrict access of others to the stored information, whether data is encrypted and password protected, and determining what will happen to the information in the event the lawyer defaults on an agreement with the third party provider or terminates the relationship with the third party provider); Me. Bd. of Bar Overseers Ethics Op. 194 (2008), *available at* http://www.maine.gov/tools/whatsnew/index.php?topic=mebar_overseers_ethics_opinions &id=86894&v=article; Mass. Bar Ass'n Comm. on Prof'l Ethics Op. 12-03 (2012), *available at* http://www.massbar.org/publications/ethics-opinions/2010-2019/2012/opinion-12-03; State Bar of Nev. Comm. on Ethics and Prof'l Responsibility, Formal Op. 33 (2006), *available at* http://ftp.documation.com/references/ABA10a/PDfs/3_12.pdf (Attorney may store client files electronically on a remote server controlled by a third party as long as he takes precautions to safeguard confidential information such as obtaining the third party's agreement to maintain confidentiality); N.H. Bar Ass'n Ethics Comm. Op. 2012-13/4 (2013), *available at* http://www.nhbar.org/legal-links/Ethics-Opinion-2012-13_04.asp; N.J. Advisory Comm. on Prof'l Ethics Op. 701 (2006), *available at* http://www.judiciary.state.nj.us/notices/ ethics/ACPE_Opinion701_ElectronicStorage_ 12022005.pdf; N.Y. State Bar Ass'n Comm. on Prof'l Ethics Op. 842 (2010), *available at* http://old.nysba.org/AM/Template.cfm?Section=Ethics_Opinions&ContentID=140010&te mplate=/CM/ContentDisplay.cfm (Attorney may use online computer data storage system to store client files provided she takes reasonable care to maintain confidentiality, and stay informed of both technological advances that could affect confidentiality and changes in the law that could affect privilege); N.C. State Bar, Formal Op. 2011-6 (2012), *available at* http://www.ncbar.com/ethics/printopinion.asp?id=855; Or. State Bar, Formal Op. 2011-188 (2011), *available at* http://www.osbar.org/_docs/ethics/2011-188.pdf; Pa. Bar Ass'n on Legal Ethics and Prof'l Responsibility Op. 2011-200 (2011), *available at* http://www.slaw.ca/wp-content/uploads/2011/11/2011-200-Cloud-Computing.pdf ("An attorney may ethically allow client confidential material to be stored in 'the cloud' provided

attack scenarios like the Billiton-Potash deal, cloud computing is relatively safe and offers tremendous advantages. Attorneys should be able to take advantage of the technology with confidence, and with clear, simple ethical guidance.

To that end, this paper aims to isolate the pertinent ethical issues of cloud computing and chart a more sensible path forward for lawyers. Part II briefly introduces the concept of cloud computing. Part III discusses the lawyer's duties of confidentiality, of competence, to protect client property, and to oversee non-lawyers who are providing assistance. Part III also examines the application of these duties by the various state bar associations to the problem of cloud computing. Part IV looks at sample terms of use of some of the more popular vendors. Part V suggests that securing informed consent, employing specialty cloud providers, and purchasing cyber insurance provide more practical ways to ensure a lawyer doesn't run afoul of his ethical obligations. The Conclusion is at Part VI.

II. WELCOME TO THE CLOUD

The idea of cloud computing is not new. Although credit is normally given to Dr. Ramnath K. Chellappa of Emory University for coining the term "cloud computing" in 1997, the underlying concept, known as "time sharing," dates back to the Fifties, when companies began designing ways to save resources by allowing multiple users to access a computer at the same time.[11] In 1961 Professor John McCarthy suggested that "[c]omputing may someday be organized as a public utility just as the telephone system is a public utility," and in 1969 J.C.R. Licklider introduced an idea for "an intergalactic computer network" in which programs and data could be accessed from anywhere.[12] By the time Google

---

he 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"); Vt. Bar Ass'n Ethics Op. 2010-6 (2010), *available at* https://www.vtbar.org/FOR%20ATTORNEYS/Advisory%20Ethics%20Opinion.aspx.

11. *See, e.g.,* Neha Prakash, *Did You Know Cloud Computing Has Been Around Since the '50s?*, MASHABLE (Oct. 26, 2012), http://mashable.com/2012/10/26/cloud-history/ ("In 1997, professor Ramnath Chellappa was the first to use the term 'cloud computing.' Then, in 1999, Salesforce.com became the first site to deliver applications and software over the Internet."); *30 years of accumulation: A timeline of cloud computing*, GCN (May 30, 2013), http://gcn.com/articles/2013/05/30/gcn30-timeline-cloud.aspx ("1997: The term 'cloud computing' is coined by University of Texas professor Ramnath Chellappa in a talk on a "new computing paradigm.'").

12. McCarthy explained that "[e]ach subscriber needs to pay only for the capacity he actually uses, but he has access to all programming languages characteristic of a very large system . . . . Certain subscribers might offer service to other subscribers . . . . The

and Microsoft rolled out cloud computing services in 2008, McCarthy's and Licklider's visions were close to realized.[13] Various types of cloud computing are now widely available at low cost, and a wide swath of the public has taken advantage. It is estimated that, as of early 2013, more than half of all businesses in the U.S. are utilizing some form of cloud computing, and the total number of cloud users at the end of 2012 is estimated to be near 500 million.[14] Some are forecasting 1.3 billion cloud users by the end of 2017.[15]

So what exactly is "the cloud"? IBM defines "[c]loud computing, often referred to as simply 'the cloud,' [as] the delivery of on-demand computing resources—everything from applications to data centers—over the Internet on a pay-for-use basis."[16] The Florida State Bar Association paints a lawyer-specific picture that will likely look familiar:

> Cloud computing involves use of an outside service provider which

---

computer utility could become the basis of a new and important industry." Simson Garfinkel, *The Cloud Imperative*, MIT TECH. REV. (Oct. 3, 2011), http://www.technologyreview.com/news/425623/the-cloud-imperative/. For a discussion of Licklider, *see Computing's Johnny Appleseed*. M. Mitchell Waldrop, *Computing's Johnny Appleseed*, MIT TECH. REV. (Jan. 1, 2000), http://www.technologyreview.com/ featuredstory/400633/computings-johnny-appleseed/.

13. *See* Prakash, *supra* note 12.

14. Jagdish Rebello, *Consumers Aggressively Migrate Data to Cloud Storage in First Half of 2012*, ISUPPLI MKT. RESEARCH (Oct. 15, 2012), http://www.isuppli.com/Mobile-and-Wireless-Communications/News/Pages/Consumers-Aggressively-Migrate-Data-to-Cloud-Storage-in-First-Half-of-2012.aspx; *see* Cohen, *supra* note 7.

15. As evidence of cloud computing's popularity, there are also the valuations of the top 15 cloud computing companies, all of which were recently estimated to be worth over $1 billion, and the largest of which, Salesforce.com, was estimated to be worth $25.5 billion. Julie Bort, *The 15 Most Valuable Cloud Computing Companies in the World Are Worth Way More Than You'd Think*, BUS. INSIDER (Jul. 29, 2013 9:17 PM), http://www.businessinsider.com/the-15-most-valuable-cloud-computing-companies-2013-7?op=1. Also, there is the recent estimate that more than half of all U.S. businesses now utilize cloud computing services. Cohen, *supra* note 7. And there is the growth in the actual size of the cloud. Technology website MASHABLE estimated in late 2012 that the total amount of storage space currently available in the cloud is at least one exabyte. *Id.* How much space is that? According to a 2003 study from the University of California at Berkeley, it's enough to store one-fifth of all the words ever spoken in human history. UNIVERSITY OF CALIFORNIA AT BERKELEY, SCHOOL OF MANAGEMENT SYSTEMS, HOW MUCH INFORMATION CASE STUDY (2003), *available at* http://www2.sims.berkeley.edu/research/projects/how-much-info-2003/. For examples of the sizes of cloud computing contracts being inked, *see Sources: Amazon and CIA ink cloud deal*. Frank Konkel, *Sources: Amazon and CIA ink cloud deal*, FCW (Mar. 18, 2013), http://fcw.com/ articles/2013/03/18/amazon-cia-cloud.aspx; *See also* Kathleen Miller & Chris Strohm, *IBM Wins Its Largest U.S. Cloud-Computing Contract*, BLOOMBERG (Aug. 14, 2013, 11:00 PM), http://www.bloomberg.com/news/2013-08-15/ibm-wins-its-largest-u-s-cloud-computing-contract .html.

16. *IBM Cloud,* IBM, http://www.ibm.com/cloud-computing/us/en/ what-is-cloud-computing.html (last visited June 5, 2014).

> provides computing software and data storage from a remote location that the lawyer accesses over the Internet via a web browser, such as Internet Explorer, or via an "app" on smart phones and tablets. The lawyer's files are stored at the service provider's remote server(s). The lawyer can thus access the lawyer's files from any computer or smart device and can share files with others.[17]

Cloud computing activities are generally categorized as Software as a Service (SaaS), in which software runs on remote computers; Platform as a Service (PaaS), in which operating systems and associated services are delivered over the internet; or Infrastructure as a Service (IaaS), in which users outsource equipment, including storage, hardware, and servers, used to support operations.[18] Of these categories, SaaS, which includes Internet email, and IaaS, which includes cloud storage services like Google Drive, are of particular concern to an attorney.[19]

Of course there are dangers unique to cloud computing, and there are plenty of headlines, similar to the Billiton-Potash breach, to illustrate the point. In 2007, for example, the hack of retailers TJ Maxx and Marshalls compromised the credit and debit card data of approximately 45 million shoppers. [20] In 2010, after ceasing to do business with the media organization WikiLeaks, both PayPal and Amazon were the subject of cyber-attacks by hacker groups.[21] In 2011 Sony's PlayStation network, which at the time hosted 77 million user accounts, was

---

17. Fla. Bar Ethics Op. 12-3 (2013), *available at* https://www.floridabar.org/__85256AA9005B9F25.nsf/0/9DA5423ABE78318685257B0100535ADD?OpenDocument.

18. Although at least one of the state bar ethics opinions mentioned below conceives, incorrectly, of SaaS and IaaS as separate from online email and data storage, and others use the terms "cloud computing" and "SaaS" interchangeably, this paper dispenses with technical terms and uses "cloud computing" to refer to all types of remote computing, with an eye towards internet email and document storage specifically. Margaret Rouse, *SPI model (SaaS, PaaS, IaaS)*, SEARCH CLOUD COMPUTING (Feb. 3, 2012), http://searchcloudcomputing.techtarget.com/definition/SPI-model.

19. These three services, together, are known as the "SPI" (software, platforms, and infrastructure) model. *Id*. In addition to the divisions between these three "service models," cloud computing "deployment models" are also divided between "public cloud," in which a cloud infrastructure is available for open use by the public; "private cloud," used exclusively by a single organization; and "hybrid cloud." IBM *Cloud,* IBM, http://www.ibm.com/cloud-computing/us/en/ what-is-cloud-computing.html (last visited June 5, 2014).

20. Mark Jewell, *T.J. Maxx theft believed largest hack ever,* NBC NEWS (Mar. 30, 2007, 11:12 AM), http://www.nbcnews.com/id/17871485/ns/technology_and_science-security/t/tj-maxx-theft-believ ed-largest-hack-ever/#.UiUkA2Q5xdc.

21. Ian Shapira, *Amazon, PayPal fend off hacker attacks over WikiLeaks*, WASH. POST (Dec. 9, 2010 8:30 PM), http://www.washingtonpost.com/wp-dyn/content/article/2010/12/09/AR2010120905893.html.

breached by hackers who stole credit and debit card information, inflicting damage estimated at $1-2 billion.[22] In late 2013 Target revealed that hackers had acquired the names, addresses, and phone numbers of 70 million customers.[23] And just a few weeks later the popular social media company, Snapchat, announced that 4.6 million users' personal information had been compromised.[24]

Perhaps because of their heightened professional obligations, lawyers have been more reluctant than others to avail themselves to use cloud computing services.[25] But this is changing. The 2012 ABA Legal Tech Study indicates that 29 percent of solo practitioners, and 26 percent of firms with two to nine attorneys, are using cloud computing, and, while only fifteen percent of firms with more than 500 attorneys are doing so, 50 percent of all firms reported an increase in the use of cloud computing services from the previous year.[26] When asked whether cloud computing services would eventually replace on-site computing entirely, only 16 percent of respondents said it would not.[27]

So if cloud computing is the emerging new normal, how should an attorney navigate the very real risks associated with it? How can she store client information online or use internet-based discovery tools and maintain her ethical obligations of confidentiality and competence? How can she store documents with a third party and maintain her profes-

---

22. Liana B. Baker & Jim Finkle, *Sony PlayStation suffers massive data breach*, REUTERS (Apr. 26, 2011), *available at* http://www.reuters.com/article/2011/04/26/us-sony-stoldendata-idUSTRE73P6WB20110426.

23. Michael Riley, et. al., *Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It*, BLOOMBERG BUS. WK. (Mar. 13, 2014), http://www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data.

24. Brian Fung, *A Snapchat security breach affects 4.6 million users. Did snapchat drag its feet on a fix?*, WASH. POST (Jan. 1, 2014), http://www.washingtonpost.com/blogs/the-switch/wp/2014/ 01/01/a-snapchat-security-breach-affects-4-6-million-users-did-snapchat-drag-its-feet-on-a-fix/.

25. *See* Black, *supra* note 8. ("So, overall the forecast for the use of cloud computing by lawyers is a good one and the scales are now tipping in favor of this 21st century technology. Although the legal profession was initially hesitant to embrace the benefits of cloud computing, it is perceived by many businesses, both legal and non-legal alike, to be a viable and appealing alternative to traditional server-based computing."); Stephanie L. Kimbro & Tom Mighell, *Popular Cloud Computing Services for Lawyers: Practice Management Online*, LAW PRACTICE (2011), *available at* http://www.americanbar.org/publications/law_practice_magazine/2011/september_october/popular_cloud_computing_services_for_lawyers.html (listing multiple providers available for cloud services including time, billing and invoicing; electronic signatures; case and client management; document management; virtual law office services; project management; online document storage and backup; remote access; and encrypted email and document exchange).

26. *See* Black, *supra* note 8.

27. *Id.*

sional duties to safeguard client property or comply with her obligations to utilize non-lawyer assistance responsibly?

III. THE ETHICS OF CLOUD COMPUTING

So far, all sixteen of the state bar ethics committees that have taken up cloud computing[28] have decided that an attorney may use the internet to communicate with clients and store client files, provided that the attorney uses reasonable care.[29] Unfortunately, most of the opinions

---

28. The question of cloud computing is framed slightly differently by each state. Maine, for example, asks about "the ethical propriety of using third party vendors to process and store electronically held firm data." Me. Bd. of Bar Overseers Ethics Op. 194 (2008), *available at* http://www.maine.gov/tools/whatsnew/index.php?topic=mebar_overseers_ethics_opinions &id=86894&v=article. New Jersey asks "whether an attorney may store documents in PDF format in the cloud." N.J. Advisory Comm. on Prof'l Ethics Op. 701 (2006), *available at* http://www.judiciary.state.nj.us/notices/ ethics/ACPE_Opinion701_ElectronicStorage_ 12022005.pdf. And New York discusses the whether an attorney can "use an online system to store a client's confidential information without violating the duty of confidentiality or any other duty." N.Y. State Bar Ass'n Comm. on Prof'l Ethics Op. 842 (2010), *available at* http://old.nysba.org/AM/Template.cfm?Section=Ethics_Opinions&ContentID=140010&te mplate=/CM/ContentDisplay.cfm.

29. *See* Ala. State Bar Ethics Op. 2010-02 (2010), *available at* http://www.alabar.org/ogc/PDF/2010-02.pdf (Attorney can outsource storage of client files if he takes reasonable steps to make sure data is protected); Az. State Bar Ethics Op. 09-04 (2009), *available at* http://www.azbar.org/Ethics/EthicsOpinions/ViewEthicsOpinion?id=704 (Attorney can use online file storage and retrieval system that enables clients to access their files over the Internet, as long as she takes reasonable precautions to protect confidentiality of the information); Cal. State Bar, Formal Op. 2010-179 (2010), *available at* http://ethics.calbar.ca.gov/LinkClick.aspx?fileticket= wmqECiHp7h4%3D&tabid=837; Fla. Ethics Op. 12-3, *available at* https://www.floridabar.org/__85256AA9005B9F25.nsf/0/9DA5423ABE78318685257B0100 535ADD?OpenDocument; Iowa State Bar Comm. on Ethics, Formal Op. 11-01 (2011), *available at* http://www.iabar.net/ethics.nsf/e61beed77a2 15f6686256497004ce492/02566cb52c2192e28625791f00834cdb/$FILE/Ethics%20Opinion %2011-01%20--%20Software%20as%20a%20Service%20-%20Cloud%20Computing.pdf (Appropriate due diligence a lawyer should perform before storing files electronically with a third party using SaaS (cloud computing), includes determining that attorney will have adequate access to the stored information and will be able to restrict access of others to the stored information, whether data is encrypted and password protected, and determining what will happen to the information in the event the lawyer defaults on an agreement with the third party provider or terminates the relationship with the third party provider); Me. Bd. of Bar Overseers Ethics Op. 194 (2008), *available at* http://www.maine.gov/tools/whatsnew/index.php?topic=mebar_overseers_ethics_opinions &id=86894&v=article; Mass. Bar Ass'n Comm. on Prof'l Ethics Op. 12-03 (2012), *available at* http://www.massbar.org/publications/ethics-opinions/2010-2019/2012/opinion-12-03;

take an unnecessarily cautious, if not altogether suspicious, attitude towards cloud computing, place unrealistic demands on attorneys, and are naive about the attorney's ability to negotiate terms with cloud vendors. Although each state bar promulgates its own set of rules of professional responsibility, they contemplate duties similar, if not identical, to those found in the Model Rules of Professional Conduct. Of these duties, four are implicated by cloud computing: confidentiality (Model Rule 1.6), competence (Model Rule 1.1), safeguarding client property (Model Rule 5.3), and non-lawyer assistance (Model Rule 5.3). Accordingly, analyses of some of the applicable state bar opinions are also addressed below under these headings.

A. CONFIDENTIALITY (MODEL RULE 1.6)

It is axiomatic that, in the words of Model Rule 1.6(a), "[a] lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent [or] the disclosure is impliedly authorized in order to carry out the representation."[30] But the lawyer's duty of confidentiality is more than a prohibition against revealing a client's secrets; he is required to ensure that no one else does, either. Model Rule 1.6(c) states that "[a] lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthor-

---

State Bar of Nev. Comm. on Ethics and Prof'l Responsibility, Formal Op. 33 (2006), *available at* http://ftp.documation.com/references/ABA10a/PDfs/3_12.pdf (Attorney may store client files electronically on a remote server controlled by a third party as long as he takes precautions to safeguard confidential information such as obtaining the third party's agreement to maintain confidentiality); N.H. Bar Ass'n Ethics Comm. Op. 2012-13/4 (2013), *available at* http://www.nhbar.org/legal-links/Ethics-Opinion-2012-13_04.asp; N.J. Advisory Comm. on Prof'l Ethics Op. 701 (2006), *available at* http://www.judiciary.state.nj.us/notices/ ethics/ACPE_Opinion701_ElectronicStorage_12022005.pdf; N.Y. State Bar Ass'n Comm. on Prof'l Ethics Op. 842 (2010), *available at* http://old.nysba.org/AM/Template.cfm?Section=Ethics_Opinions&ContentID=140010&template=/CM/ContentDisplay.cfm (Attorney may use online computer data storage system to store client files provided she takes reasonable care to maintain confidentiality, and stay informed of both technological advances that could affect confidentiality and changes in the law that could affect privilege); N.C. State Bar, Formal Op. 2011-6 (2012), *available at* http://www.ncbar.com/ethics/printopinion.asp?id=855; Or. State Bar, Formal Op. 2011-188 (2011), *available at* http://www.osbar.org/_docs/ethics/2011-188.pdf; Pa. Bar Ass'n on Legal Ethics and Prof'l Responsibility Op. 2011-200 (2011), *available at* http://www.slaw.ca/wp-content/uploads/2011/11/2011-200-Cloud-Computing.pdf ("An attorney may ethically allow client confidential material to be stored in 'the cloud' provided he 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"); Vt. Bar Ass'n Ethics Op. 2010-6 (2010), *available at* https://www.vtbar.org/FOR%20ATTORNEYS/Advisory%20Ethics%20Opinion.aspx.

30. Model Rules of Prof'l Conduct R. 1.6(a) (2012).

ized access to, information relating to the representation of a client,"[31] and Comment 18 explains that:

> [p]aragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision.

What constitutes "reasonable efforts" to prevent disclosure? Comment 18 says that the lawyer's efforts will be judged on a variety of factors, including "the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients…."[32]

A central concern, when it comes to cloud computing, is confidentiality. Accordingly, every state bar ethics committee that has taken up the issue has addressed the duty to maintain client confidences. The touchstones of these analyses have generally been, as in Model Rule 1.6, the reasonableness of the lawyer's efforts to prevent disclosure. In Alabama, for example, "[a] lawyer may also choose to store or 'back-up' client files via a third-party provider or internet-based server, provided that the lawyer exercises reasonable care in doing so,"[33] and in New York "[a] lawyer may use an online 'cloud' computer data backup system to store client files provided that the lawyer takes reasonable care to ensure that the system is secure and that client confidentiality will be maintained."[34]

So what constitutes reasonable efforts to safeguard against disclo-

---

31. *Id.* at 1.6(c).

32. Model Rules of Prof'l Conduct R. 1.6 cmt. 18 (2012); The comment provides that:

> A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule. Whether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other law, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules.

Model Rules of Prof'l Conduct R. 1.6 cmt. 18 (2012).

33. Ala. State Bar Ethics Op. 2010-02 (2010), *available at* http://www.alabar.org/ogc/PDF/2010-02.pdf.

34. N.Y. State Bar Ass'n Comm. on Prof'l Ethics Op. 842 (2010), *available at* http://old.nysba.org/AM/Template.cfm?Section=Ethics_Opinions&ContentID=140010&template=/CM/ContentDisplay.cfm.

sure of confidential information stored in the cloud,[35] in Pennsylvania the standard of reasonable care includes no less than 33 factors.[36] Discussing every consideration which could conceivably bear on the question of cloud computing would, for the limited purposes of this paper, be a waste of time. There are however a few practical and highly relevant factors of reasonableness that recur in the opinions.

Perhaps most importantly, several of the state bar associations suggest considering the sensitivity of the client's information, a consideration which is included in Comment 18 to Rule 1.6.[37] California explains that "[t]he greater the sensitivity of the information, the less risk an attorney should take with technology. If the information is of a highly sensitive nature and there is a risk of disclosure when using a particular technology, the attorney should consider alternatives unless the client provides informed consent."[38] Massachusetts likewise mandates that an attorney "should refrain from storing or transmitting particularly sensitive client information by means of the Internet without first seeking and obtaining the client's express consent to do so."[39] Vermont reasons, "[g]iven that Cloud Computing involves storage of information in the hands of a third party, a lawyer handling particularly sensitive client property, like trade secrets may conclude after consultation with

---

35. The California State Bar is presented with a hypothetical in which an "[a]ttorney takes his laptop computer to the local coffee shop and accesses a public wireless Internet connection to conduct legal research on the matter and email Client. He also takes the laptop computer home to conduct the research and email Client from his personal wireless system." Cal. State Bar, Formal Op. 2010-179 (2010), *available at* http://ethics.calbar.ca.gov/LinkClick.aspx?fileticket= wmqECiHp7h4%3D&tabid=837. But "[r]ather than engage in a technology-by-technology analysis, which would likely become obsolete shortly," its opinion "sets forth the general analysis that an attorney should undertake when considering use of a particular form of technology." *Id.*

36. There are, as best as the authors can tell, about 13 broad headings for these factors to be considered in determining what constitutes "reasonable efforts" to ensure confidentiality: (1) backing up data, (2) installing a firewall, (3) limiting information provided to others, (4) avoiding inadvertent disclosures, (5) verifying the identity of individuals to whom the attorney provides information, (6) refusing to disclose confidential information to unauthorized individuals without client permission, (7) encrypting confidential data, (8) "implementing electronic audit trail procedures to monitor who is accessing the data," (9) creating plans to address security breaches, (10) vetting service providers and service agreements, (11) training employees, (12) storing copy of digital data onsite, and (13) having an alternate way to connect to the internet. Pa. Bar Ass'n on Legal Ethics and Prof'l Responsibility Op. 2011-200 (2011), *available at* http://www.slaw.ca/wp-content/uploads/2011/11/2011-200-Cloud-Computing.pdf.

37. Model Rules of Prof'l Conduct R. 1.6, cmt. 18 (2012).

38. Cal. State Bar, Formal Op. 2010-179 (2010), *available at* http://ethics.calbar.ca.gov/LinkClick.aspx?fileticket= wmqECiHp7h4%3D&tabid=837.

39. Mass. Bar Ass'n Comm. on Prof'l Ethics Op. 12-03 (2012), *available at* http://www.massbar.org/publications/ethics-opinions/2010-2019/2012/opinion-12-03.

the client that remote SaaS storage is not sufficiently secure."[40] Other than trade secrets, the opinions do not mention other types of sensitive information, necessarily requiring the attorney to make this a case-by-case, client-specific determination.

But another factor frequently considered by the state bars—whether an attorney has kept abreast of vendors' security measures—is new territory for many attorneys with real questions about the degree to which the vast majority of lawyers are even equipped to assess and evaluate the technical merits or demerits of such security measures. Oregon suggests that an attorney should be equipped to rate the security systems of cloud vendors:

> Although the third-party vendor may have reasonable protective measures in place to safeguard the client materials, the reasonableness of the steps taken will be measured against the technology "available at the time to secure data against unintentional disclosure." As technology advances, the third-party vendor's protective measures may become less secure or obsolete over time. Accordingly, Lawyer may be required to reevaluate the protective measures used by the third-party vendor to safeguard the client materials.[41]

But does the lawyer, as Alabama suggests, really "have a continuing duty to stay abreast of appropriate security safeguards that should be employed by . . . the third-party provider"?[42] Is an attorney equipped, as mandated by the Florida Bar, to "[i]nvestigat[e] the online data storage provider's security measures, policies, recoverability methods, and other procedures to determine if they are adequate under the circumstances"?[43] Should an attorney know how Google is defending against

---

40. The Vermont lawyer, like her counterparts in California and Pennsylvania, has a number of factors to weigh when deciding what constitutes reasonable efforts: (1) the vendor's security system; (2) what practical limits may exist to the lawyer's "ability to ensure access to, protection of, and retrieval of the data;" (3) material terms of the user agreement; (4) the vendor's commitment to protecting confidentially; (5) the nature and sensitivity of the information; (6) notice provisions if a third party seeks or gains access to the data; (7) other regulatory, compliance, and document retention obligations that may apply. The lawyer should also consider: (1) giving notice to the client about cloud usage; (2) having the vendor's security and access systems reviewed by competent technical personnel; (3) establishing a system for periodic review of the vendor's system; and (4) taking reasonable measures to stay apprised of technological developments. Vt. Bar Ass'n Ethics Op. 2010-6 (2010), *available at* https://www.vtbar.org/FOR%20ATTORNEYS/Advisory%20Ethics%20Opinion.aspx.

41. Or. State Bar, Formal Op. 2011-188 (2011), *available at* http://www.osbar.org/_docs/ethics/2011-188.pdf.

42. Ala. State Bar Ethics Op. 2010-02 (2010), *available at* http://www.alabar.org/ogc/PDF/2010-02.pdf.

43. Fla. Bar Ethics Op. 88-11 (1988), *available at*

"zombie drones," "dumpster divers," and DDOS attacks? Should she know Dropbox's emergency plans for a "zero day threat" or the difference between SAML 2.0 and ID-FF 1.2?[44] New Jersey understates the obvious when it says that "[p]roviding security on the Internet against hacking and other forms of unauthorized use has become a specialized and complex facet of the industry, and it is certainly possible that an independent ISP may more efficiently and effectively implement such security precautions."[45]

Some state bar associations suggest overcoming this obvious hurdle by hiring experts. California suggests, perhaps contradictorily, that an attorney need not master the subject of cyber security, but that, if he can't understand the basics, he should hire an expert:

> Although the Committee does not believe that attorneys must develop a mastery of the security features and deficiencies of each technology available, the duties of confidentiality and competence that attorneys owe to their clients do require a basic understanding of the electronic protections afforded by the technology they use in their practice. If the attorney lacks the necessary competence to assess the security of the technology, he or she must seek additional information or consult with someone who possesses the necessary knowledge, such as an information technology consultant.[46]

But the hiring of experts or consultants is expensive (prohibitively so for many small firms and solo practitioners), and it is not in any event necessary if state bar associations do not pull more from the Model Rules than is there. Comment 8's admonition to "keep abreast of . . . the benefits and risks associated with relevant technology" is broader, less onerous, and more reasonable than a requirement that an attorney

---

http://www.floridabar.org/tfb/tfbetopin.nsf/SearchView/ETHICS,+OPINION+88-11?opendocument.

44. *See Cyber Crime/Hacker Terminology*, GLOBAL DIGITAL FORENSICS, http://evestigate.com/cyber-crime- hacker-terms-to-know/ (last visited June 14, 2014) (providing a list of sample hacker jargon). *See, e.g.*, *Oracle Identity Federation Administrator's Guide*, ORACLE, http://docs.oracle.com/cd/E10773_01/doc/oim.1014/b25355/intro.htm (last visited June 14, 2014) (providing a sampling of cyber security technical jargon).

45. N.J. Advisory Comm. on Prof'l Ethics Op. 701 (2006), *available at* http://www.judiciary.state.nj.us/notices/ ethics/ACPE_Opinion701_ElectronicStorage_12022005.pdf. New Jersey's opinion, tellingly, but perhaps inadvertently, validates the point that lawyers are not technology experts by using the term "ISP" (internet service provider) in reference to cloud computing vendors: ("It is very possible that a firm might seek to store client sensitive data on a larger file server or a web server provided by an outside Internet Service Provider (and shared with other clients of the ISP) in order to make such information available to clients, where access to that server may not be exclusively controlled by the firm's own personnel."). *Id.*

46. Cal. State Bar, Formal Op. 2010-179 (2010), *available at* http://ethics.calbar.ca.gov/LinkClick.aspx?fileticket= wmqECiHp7h4%3D&tabid=837.

should, as New York suggests, "stay abreast of technological advances to ensure that the storage system remains sufficiently advanced to protect the client's information."[47]

Finally, there is the question of whether "reasonable efforts" to maintain confidentiality include securing an enforceable obligation on the part of the vendor to safeguard a client's data from disclosure. Some states are unsure. New York suggests half-heartedly that reasonable care "may include consideration of . . . [e]nsuring that the online data storage provider has an enforceable obligation to preserve confidentiality and security, and that the provider will notify the lawyer if served with process requiring the production of client information."[48] But in Maine, the lawyer should "[a]t a minimum . . . 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."[49] And in New Jersey "[t]he touchstone in using 'reasonable care' against unauthorized disclosure is that [] the lawyer has entrusted such documents to an outside provider under circumstances in which there is an enforceable obligation to preserve confidentiality and security."[50]

Unsurprisingly, the terms of use of popular cloud providers, as discussed below, are, to varying degrees, drafted very favorably for the cloud provider. A notable flaw of many of the State bar ethics opinions discussed above is that they maintain the unrealistic assumption that the users of cloud services (i.e., the law firms) actually have some ability to modify one-sided or onerous legal terms in the standard terms and conditions. But it does not correlate to reality to assume that a law firm—especially a small law firm or sole practitioner—can negotiate terms of use with a company the size of Dropbox, to say nothing of Microsoft and Google. Can an attorney, as Nevada recommends, "[i]nstruct[] and require[] the third party contractor to keep the information confidential and inaccessible"?[51] Only Pennsylvania acknowl-

---

47. N.Y. State Bar Ass'n Comm. on Prof'l Ethics Op. 842 (2010), *available at* http://old.nysba.org/AM/Template.cfm?Section=Ethics_Opinions&ContentID=140010&template=/CM/ContentDisplay.cfm.

48. *Id.*

49. Me. Bd. of Bar Overseers Ethics Op. 194 (2008), *available at* http://www.maine.gov/tools/whatsnew/index.php?topic=mebar_overseers_ethics_opinions&id=86894&v=article.

50. N.J. Advisory Comm. on Prof'l Ethics Op. 701 (2006), *available at* http://www.judiciary.state.nj.us/notices/ ethics/ACPE_Opinion701_ElectronicStorage_12022005.pdf.

51. State Bar of Nev. Comm. on Ethics and Prof'l Responsibility, Formal Op. 33 (2006), *available at* http://ftp.documation.com/references/ABA10a/PDfs/3_12.pdf.

edges the essential fact that "negotiating" with a cloud provider—usually, is "take it or leave it."[52]

Comment 18 says that the reasonableness of an attorney's efforts to ensure confidentiality depend on "the cost of employing additional safeguards, [and] the difficulty of implementing the safeguards."[53] Does this suggest that lower security standards may be deemed more acceptable under the Rule for solo and smaller law firms, given that they may be less able to reasonably absorb and spread those costs than a much larger law firm?[54] By overestimating both the level of an attorney's expertise and her ability to negotiate with vendors, and in some cases requiring intricate, expert analyses before using cloud computing,[55] the various ethics opinions that have been issued do not provide adequate guidance. Take the following from Massachusetts:

The foregoing policies, protections and resources are referenced by the

---

52. Pa. Bar Ass'n on Legal Ethics and Prof'l Responsibility Op. 2011-200 (2011), *available at* http://www.slaw.ca/wp-content/uploads/2011/11/2011-200-Cloud-Computing.pdf.

53. MODEL RULES OF PROF'L CONDUCT R. 1.6, cmt. 18 (2012).

54. Comment 18 also makes clear that a client may require the lawyer to implement special security measures not required by Model Rule 1.6 or may give informed consent to forgo security measures that would otherwise be required by the rule. One obvious place for the memorialization of these terms would be in the attorney-client engagement letter. But the mere execution of such an agreement alone would be insufficient, since it would be essential for the attorney to ensure not only that there was informed consent by the client, but also that there was compliance with all applicable rules, regulations and laws, including the data breach notification laws required now required in 46 of the 50 states. *See infra* Part IV.

55. Oregon, for another example, requires attorneys to consider:

(1) Inclusion in the SaaS vendor's Terms of Service or Service Level Agreement, or in a separate agreement between the SaaS vendor and the lawyer or law firm, of an agreement on how the vendor will handle confidential client information in keeping with the lawyer's professional responsibilities.

(2) If the lawyer terminates use of the SaaS product, the SaaS vendor goes out of business, or the service otherwise has a break in continuity, the law firm will have a method for retrieving the data, the data will be available in a non-proprietary format that the law firm can access, or the firm will have access to the vendor's software or source code. The SaaS vendor is contractually required to return or destroy the hosted data promptly at the request of the law firm.

(3) Careful review of the terms of the law firm's user or license agreement with the SaaS vendor including the security policy.

(4) Evaluation of the SaaS vendor's (or any third party data hosting company's) measures for safeguarding the security and confidentiality of stored data including, but not limited to, firewalls, encryption techniques, socket security features, and intrusion-detection systems.

(5) Evaluation of the extent to which the SaaS vendor backs up hosted data. Or. State Bar, Formal Op. 2011-188 (2011), *available at* http://www.osbar.org/_docs/ethics/2011-188.pdf.

> Committee solely for informational purposes. Ultimately, the question of whether the use of Google docs, or any other Internet based data storage service provider, is compatible with Lawyer's ethical obligation to protect his clients' confidential information is one that Lawyer must answer for himself based on the criteria set forth in this opinion, the information that he is reasonably able to obtain regarding the relative security of the various alternatives that are available, and his own sound professional judgment.[56]

The ethical questions in Massachusetts, it seems, are in the end left to the attorney. How can he be confident he is on solid footing in the cloud?

B. COMPETENCE (MODEL RULE 1.1)

Model Rule of Professional Responsibility 1.1 requires that a lawyer provide "competent representation" to a client. "Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation."[57] Comment 1 explains that "[i]n determining whether a lawyer employs the requisite knowledge and skill in a particular matter, relevant factors include the relative complexity and specialized nature of the matter, the lawyer's general experience, [and] the lawyer's training and experience in the field in question."[58] As discussed above, Comment 8, added with the latest round of amendments to the Model Rules, elaborates further that "[t]o maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology."[59]

For all but one of the state bar associations that have taken up the question of cloud computing, the duty of competence, when it is mentioned at all, overlaps with other duties. In Nevada, for example, the duty of competence requires a lawyer to "act competently to safeguard against inadvertent or unauthorized disclosure of confidential client information,"[60] and in California an attorney must "act[] competently to

---

56. Mass. Bar Ass'n Comm. on Prof'l Ethics Op. 12-03 (2012), *available at* http://www.massbar.org/publications/ethics-opinions/2010-2019/2012/opinion-12-03.

57. MODEL RULES OF PROF'L CONDUCT R. 1.1 (2012).

58. *Id.* at cmt. 1.

59. *Id.* at cmt. 8. *See also* Jackson, *supra* note 10; Matt Nelson, *New Changes to Model Rules a Wake-up Call for Technology Challenged Lawyers*, INSIDE COUNS. (Mar. 28, 2013), http://www.insidecounsel.com/2013/03/28/new-changes-to-model-rules-a-wake-up-call-for-tech.

60. State Bar of Nev. Comm. on Ethics and Prof'l Responsibility, Formal Op. 33 (2006), *available at* http://ftp.documation.com/references/ABA10a/PDfs/3_12.pdf.

preserve confidential client information."[61] New Hampshire gives individual treatment to the duty to "provide competent legal representation, and minimal competence requires a lawyer to perform the techniques of practice with skill."[62] But even in New Hampshire the lawyer's duty to perform competently is, ultimately, a duty to guard against the risks associated with cloud computing:

> As the revised Comment [6] to the ABA Model Rule 1.1 states, a lawyer must "keep abreast of changes in the law and its practice, including the benefits or risks associated with relevant technology." The comment was revised recently in response to "the sometimes bewildering pace of technological change," including cloud computing. A competent lawyer using cloud computing must understand and guard against the risks inherent in it.[63]

Requiring a lawyer to use technology competently is, of course, reasonable enough. But is the lawyer's duty of competence, as it relates to cloud computing, merely cautionary? Is the duty of competence, as in Oregon, merely the duty "to reasonably keep the client's information secure within a given situation"?[64] Only New Jersey conceptualizes the attorney's duty of competence as an affirmative duty to avail himself of the benefits of technology:

> The paramount consideration is the ability to represent the client competently, and given the advances of technology, a lawyer's ability

---

61. Cal. State Bar, Formal Op. 2010-179 (2010), *available at* http://ethics.calbar.ca.gov/LinkClick.aspx?fileticket= wmqECiHp7h4%3D&tabid=837. In California—the jurisdiction which, after New York, has the second highest number of attorneys on active status in the nation—the ABA Model Rules have not been expressly adopted, though they "may serve as guidelines absent on-point California authority or a conflicting state public policy." City and Cnty. of S. F. v. Cobra Solutions, Inc., 43 Cal Rptr. 3d 771, 781 (Cal. Ct. App. 2006) (*citing State Comp. Ins. Fund v. WPS, Inc.,* 82 Cal. Rptr. 2d 799 (Cal. Ct. App. 1999)); *National Lawyer Population by State*, A.B.A. (2013), *available at* http://www.americanbar.org/content/dam/aba/migrated/marketresearch/PublicDocuments/2013_natl_lawyer_by_state.authcheckdam.pdf. Yet there is still no case law, in California, which directly addresses a lawyer's obligations to maintain technological competence, nor is there any California public policy which conflicts with A.B.A. Model Rule 1.1 on Competence. As one commentator has pointed out, the adoption of firmly-established state and federal laws regarding e-discovery, the routine uses of e-filings for briefs, and other litigation-related documents in California courts, suggests that California has a policy consistent with Model Rule 1.1. *See* Andrew Vogel, *Should California Lawyers Have a Duty of 'Computence'?,* 33 L.A. CNTY. BAR ASS'N, Oct. 2013, *available at* http://www.lacba.org/showpage.cfm?pageid=15158.

62. N.H. Bar Ass'n Ethics Comm. Op. 2012-13/4 (2013), *available at* http://www.nhbar.org/legal-links/Ethics-Opinion-2012-13_04.asp.

63. *Id*.

64. Or. State Bar, Formal Op. 2011-188 (2011), *available at* http://www.osbar.org/_docs/ethics/2011-188.pdf.

> to discharge those duties may very well be enhanced by having client documents available in an electronic form that can be transmitted to him instantaneously through the Internet. We also note the recent phenomenon of making client documents available to the client through a secure website. This also has the potential of enhancing communications between lawyer and client, and promotes the values embraced in RPC 1.4.[65]

With this excerpt, New Jersey presents a compelling proposition: The duty of competence, as it relates to cloud computing, must require, in order to avoid being rendered useless, more than *competently* maintaining the duty of confidentiality or *competently* overseeing nonlawyers. Competence requires that an attorney avail herself of technologies that allow her to more efficiently and effectively represent her client, provided she can do so without compromising her other obligations. This is plain in the text of Comment 8 to Rule 1.1, which counsels that a lawyer "keep abreast" not only of "risks associated with relevant technology," but also of *benefits*.[66] Does a lawyer perform competently by continuing in 2014—with cloud computing, and all its benefits, so widely and cheaply available—to store documents, to correspond with clients, to otherwise run her practice as if it's 1995? Cloud computing offers tremendous advantages to an attorney, and the lawyer's duty of competence requires him her, if the new Comment 8 to Rule 1.1 has any meaning, to consider the benefits of using it.

C. CLIENT PROPERTY (MODEL RULE 1.15)

Model Rule 1.15(a) creates an express fiduciary obligation of attorneys to safeguard client property, including client documents. The rule states that "[a] lawyer shall hold property of clients or third persons that is in a lawyer's possession in connection with a representation separate from the lawyer's own property" and that such property "shall be identified as such and appropriately safeguarded."[67] An attorney must also keep "[c]omplete records" of the client's property and "preserve [the records] for a period of [five years] after termination of the representation."[68] So what constitutes appropriate safeguards for attorney-client

---

65. N.J. Advisory Comm. on Prof'l Ethics Op. 701 (2006), *available at* http://www.judiciary.state.nj.us/notices/ ethics/ACPE_Opinion701_ElectronicStorage_12022005.pdf.

66. MODEL RULES OF PROF'L CONDUCT R.1.1, cmt. 8 (2012).

67. MODEL RULES OF PROF'L CONDUCT R. 1.15(a) (2002).

68. MODEL RULES OF PROF'L CONDUCT R. 1.15(a) (2002); The entire paragraph states that:

> [A] lawyer shall hold property of clients or third persons that is in a lawyer's

privileged, client confidential documents, or other related communications that are stored on the "cloud"?

Only a few of the opinions address the duty to safeguard client property, and all but one of these offer little guidance. Alabama and New Jersey note that if an attorney scans hard copies of client files and uploads them in electronic format, he must keep the hard copies to meet Rule 1.15's requirement.[69] Iowa counsels attorneys to ask, among other questions, whether the cloud provider's "[end user license agreement] grant[s] them proprietary or user rights over my data," but does not say whether the cloud provider's ownership of data is a deal breaker.[70] North Carolina notes without discussion that "Rule 1.15 requires a lawyer to preserve client property, including information in a client's file such as client documents and lawyer work product, from risk of loss due to destruction, degradation, or loss."[71] Pennsylvania requires the attorney to ask whether "the Service Level Agreement clearly states that the attorney owns the data."[72] New Hampshire goes a step further, requir-

---

> possession in connection with a representation separate from the lawyer's own property. Funds shall be kept in a separate account maintained in the state where the lawyer's office is situated, or elsewhere with the consent of the client or third person. Other property shall be identified as such and appropriately safeguarded. Complete records of such account funds and other property shall be kept by the lawyer and shall be preserved for a period of [five years] after termination of the representation.

Model Rules of Prof'l Conduct R. 1.15(a) (2002).

69. Ala. State Bar Ethics Op. 2010-02 (2010), *available at* http://www.alabar.org/ogc/PDF/2010-02.pdf ("However, the best practice is that the lawyer should never destroy originals of Category 1 property. Where destruction is necessary and appropriate, the lawyer should deliver the original to the client or deposit it with the court. Examples of such property include, but are not limited to: wills, powers of attorney, advance healthcare directives, other executed estate planning documents, stock certificates, bonds, cash, negotiable instruments, certificates of title, abstracts of title, deeds, official corporate or other business and financial records, and settlement agreements."); N.J. Advisory Comm. on Prof'l Ethics Op. 701 (2006), *available at* http://www.judiciary.state.nj.us/notices/ ethics/ACPE_Opinion701_ElectronicStorage_ 12022005.pdf ("'Original wills, trusts, deeds, executed contracts, corporate bylaws and minutes are but a few examples of documents which constitute client property.' Such documents cannot be preserved within the meaning of RPC 1.15 merely by digitizing them in electronic form, and we do not understand the inquirer to suggest otherwise, since he acknowledges his obligation to maintain the originals of such documents in a separate file.") (quoting N.J. Advisory Comm. on Prof'l Ethics Op. 691 (2001)).

70. Iowa State Bar Comm. on Ethics, Formal Op. 11-01 (2011), *available at* http://www.iabar.net/ethics.nsf/e61beed77a2 15f6686256497004ce492/02566cb52c2192e28625791f00834cdb/$FILE/Ethics%20Opinion %2011-01%20--%20Software%20as%20a%20Service%20-%20Cloud%20Computing.pdf.

71. N.C. State Bar, Formal Op. 2011-6 (2012), *available at* http://www.ncbar.com/ethics/printopinion.asp?id=855.

72. Pa. Bar Ass'n on Legal Ethics and Prof'l Responsibility Op. 2011-200 (2011), *available at* http://www.slaw.ca/wp-content/uploads/2011/11/2011-200-Cloud-

ing not only that "the provider may not 'own' the data stored in the cloud," but that an attorney must ensure that all of the client's information is deleted from the third party's servers once representation has ended.[73]

The ABA has suggested a hard and fast rule against third party ownership.[74] This does not currently pose a problem for attorneys, as there are a number of reputable cloud providers who do not claim ownership of data uploaded to their servers. However, what happens to the data after representation has ended is, as discussed below, a matter on which attorneys are largely at the mercy of providers.[75]

D. NON-LAWYER ASSISTANCE (MODEL RULE 5.3)

Model Rule 5.3 provides that lawyers with managerial authority or direct supervisory authority over a non-lawyer must make "reasonable efforts" to ensure that the non-lawyer's assistance meets the lawyer's professional obligations.[76] Specifically, this Rule explains that the lawyer is responsible for the conduct of the non-lawyer if:

> (1) the lawyer orders or, with the knowledge of the specific conduct, ratifies the conduct involved; or (2) the lawyer is a partner or has comparable managerial authority in the law firm in which the person

---

Computing.pdf.

73. N.H. Bar Ass'n Ethics Comm. Op. 2012-13/4 (2013), *available at* http://www.nhbar.org/legal-links/Ethics-Opinion-2012-13_04.asp;

> The data must be returned to the client and deleted from the cloud after representation is concluded or when the lawyer decides to no longer to preserve the file: in either case, the lawyer must know at all times where sensitive client information is stored, be it in the cloud or elsewhere.

N.H. Bar Ass'n Ethics Comm. Op. 2012-13/4 (2013), *available at* http://www.nhbar.org/legal-links/Ethics-Opinion-2012-13_04.asp.

74. *Evaluating cloud-computing providers*, YOUR ABA (June 2012), http://www.americanbar.org/ newsletter/publications/youraba/201206article12.html. "You'll also want to verify that you retain ownership of your data. Some free service providers have been known to claim that all data uploaded into their system are their property—an unacceptable scenario when it comes to client files." *Id.*

75. *See* State Bar of Nev. Comm. on Ethics and Prof'l Responsibility, Formal Op. 33 (2006), *available at* http://ftp.documation.com/references/ABA10a/PDfs/3_12.pdf; N.H. Bar Ass'n Ethics Comm. Op. 2012-13/4 (2013), *available at* http://www.nhbar.org/legal-links/Ethics-Opinion-2012-13_04.asp; *see infra* notes 105-06.

76. MODEL RULES OF PROF'L CONDUCT R. 5.3 (2012). Notably, in these latest revisions to the model rules, the language in this Model Rule 5.3 deleted the phrase "Assistant" and substituted in the phrase "Assistance" to capture a broader category of groups (including technology vendors, such as cloud computing) that provide support to attorneys beyond the traditional, and more narrowly-defined paralegal, legal assistant and legal secretary. *Id.*

> is employed, or has direct supervisory authority over the person, and knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action.[77]

Comment 3 to this Rule, which discusses the use of non-lawyers outside of the firm, expressly condones "using an Internet-based service to store client information," provided the attorney "make[s] reasonable efforts to ensure that the services are provided in a manner that is compatible with the lawyer's professional obligations."[78] What constitutes "reasonable efforts"? According to Comment 3:

> The extent of this obligation will depend on the circumstances, including the education, experience and reputation of the non-lawyer; the nature of the services involved; the terms of any arrangements concerning the protection of client information; and the legal and ethical environments of the jurisdictions in which the services will be performed, particularly with regard to confidentiality.[79]

So what can an attorney really do to "oversee" the conduct of a company like Google or Microsoft or Go Daddy? Should an attorney seek out a smaller vendor with whom she can work more closely? Does Comment 3's consideration of the "education, experience and reputation of the non-lawyer" counsel in favor of larger, more popular cloud providers, who are likely to have more robust security in place, but with whom the attorney will not realistically be able to negotiate?

> Because cloud computing involves the use of a third party as a provider of services and involves the storage and use of data at a remote location that is also used by others outside an individual law firm, the use of cloud computing raises ethics concerns of … proper supervision of non-lawyers.[80]

The handful of opinions that address the issue are unhelpful. Both Maine and New Hampshire fold the duty to oversee non-lawyers into the duty to maintain confidentiality. Maine, for example, states:

> Clearly, when employing any outside contractor to perform law--related services, the lawyer does not directly train, monitor, and discipline the employees of the service provider; however, the lawyer retains the obligation to ensure that appropriate standards concerning client confidentiality are maintained by the contractor. The precise parameters of what constitutes "appropriate standards" are not defined in the rules or opinions, but are based on reasonable efforts to

---

77. *Id.*

78. *Id.* at cmt. 3.

79. *Id.*

80. Fla. Bar Ethics Op. 12-3 (2013), *available at* https://www.floridabar.org/__85256AA9005B9F25.nsf/0/9DA5423ABE78318685257B0100535ADD?OpenDocument.

> prevent the disclosure of confidential information.81

Moreover, New Hampshire explicitly avoids addressing the questions raised by Rule 5.3 regarding "the extent of [the lawyer's] obligation" as it is affected by the relative skill of the vendor:

> a provider of cloud computing services is, in effect, a non-lawyer retained by a lawyer. As a result, the lawyer must make reasonable efforts to ensure that the provider understands and is capable of complying with its obligation to act in a manner compatible with the lawyer's own professional responsibilities. N.H. Rule 5.3 (a)…[But w]hich providers of cloud computing may be used and what security measures the provider must take are beyond the scope of this opinion.[82]

Likewise, North Carolina reasons that the "extent of this obligation when using a SaaS vendor to store and manipulate confidential client information will depend upon the experience, stability, and reputation of the vendor," but does not say anything further about how these factors influence the lawyer's analysis.[83] Oregon offers more concrete guidance, proposing that the attorney determine whether a vendor's practices are in accordance with "industry standards."[84]

But how much can an attorney really "oversee" her cloud vendor? The opinions that evaluate the issue tend to overstate the attorney's power to negotiate. Pennsylvania acknowledges that cloud vendors' terms are usually "take it or leave it," but then goes on to suggest, without citation, that "competition in the 'cloud computing' field is now causing vendors to consider altering terms" and that an attorney may seek "a specific agreement [from the vendor] to comply with all ethical guide-

---

81. Me. Bd. of Bar Overseers Ethics Op. 194 (2008), *available at* http://www.maine.gov/tools/whatsnew/index.php?topic=mebar_overseers_ethics_opinions&id=86894&v=article.

82. N.H. Bar Ass'n Ethics Comm. Op. 2012-13/4 (2013), *available at* http://www.nhbar.org/legal-links/Ethics-Opinion-2012-13_04.asp.

83. N.C. State Bar, Formal Op. 2011-6 (2012), *available at* http://www.ncbar.com/ethics/printopinion.asp?id=855.

84. Or. State Bar, Formal Op. 2011-188 (2011), available *at* http://www.osbar.org/_docs/ethics/2011-188.pdf. "Lawyer may store client materials on a third-party server so long as Lawyer 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 requirements imposed on the Lawyer by the Oregon RPCs." *Id.*

lines…"[85] The truth is an attorney will be able to do no such thing with the most popular cloud vendors. The various state bar associations skip over this essential dilemma: using a vendor with whom the attorney can negotiate a special agreement will mean foregoing the "experience, stability, and reputation" of larger vendors like Google and Microsoft or any other known, reputable company.

IV. VENDORS' TERMS OF SERVICE

Hence, if an attorney entering the cloud decides to go with a larger, more reputable vendor, what is she likely to find in their terms of service? For example, when Google launched Google Drive, a new version of its cloud storage service, tech enthusiasts took another look at the company's privacy policies, which had also been updated less than two months earlier.[86] One particular provision in Google's omnibus policy, although it was not new language, continued to stand out:

> When you upload or otherwise submit content to our Services, you give Google (and those we work with) a worldwide license to use, host, store, reproduce, modify, create derivative works (such as those resulting from translations, adaptations or other changes we make so that your content works better with our Services), communicate, publish, publicly perform, publicly display and distribute such content.[87]

Even though Google's terms elsewhere assure users that, as far as ownership rights go, "what belongs to you stays yours," the licensing provision seems to give Google the right to do with uploaded content just about whatever they want. As one observer put it, the provision "conjures up visions of Google employees acting out your screenplay at their next all-hands meeting."[88]

For now, the terms of use of preeminent cloud storage providers are strikingly similar.[89] Google Drive, Microsoft's OneDrive, and Dropbox,

---

85. Pa. Bar Ass'n on Legal Ethics and Prof'l Responsibility Op. 2011-200 (2011), *available at* http://www.slaw.ca/wp-content/uploads/2011/11/2011-200-Cloud-Computing.pdf.

86. For the last three versions of Google's terms of use, *see Updates: Terms of Service*, GOOGLE, http://www.google.com/policies/terms/archive/ (last visited June 5, 2014). For Google's announcement of Drive's launch, *see Introducing Google Drive...yes, really*, GOOGLE BLOG (Apr. 24, 2012), http://googleblog.blogspot.com/2012/04/introducing-google-drive-yes-really.html.

87. *Terms of Service*, GOOGLE, *supra* note 86.

88. Leslie Meredith, *Does Google Drive own your data? Policy actually no worse than rivals*, FOX NEWS (Apr. 25, 2012), http://www.foxnews.com/tech/2012/04/25/does-google-drive-own-your-data-policy-actually-no-worse-than-rivals/.

89. What should an attorney look for in vendors' terms of service? "Of particular practical assistance is Iowa Ethics Opinion 11-01. Iowa State Bar Comm. on Ethics, Formal Op. 11-01 (2011), *available at* http://www.iabar.net/ethics.nsf/e61beed77a2

which are the most popular cloud storage providers on the internet today, all leave ownership of uploaded content with the user. Google says, "You retain ownership of any intellectual property rights that you hold in that content. In short, what belongs to you stays yours."[90] Microsoft says that "Your content remains your content, and you are responsible for it."[91] And Dropbox reminds you, casually, that "You retain full ownership to your stuff."[92] While Google's licensing provision may have been, as some commentators noted, poorly written by overprotective lawyers, it is not much different from the terms offered from its competitors. Dropbox's terms sound friendlier, but if Google includes a laundry list of what a user is allowing it to do, Dropbox's terms are at least as permissive for vagueness. The relevant portions say:

> We may need your permission to do things you ask us to do with your stuff, for example, hosting your files, or sharing them at your direction…You give us the permissions we need to do those things solely to provide the Services. This permission also extends to trusted third parties we work with to provide the Services, for example Amazon, which provides our storage space (again, only to provide the Services).[93]

15f6686256497004ce492/02566cb52c2192e28625791f00834cdb/$FILE/Ethics%20Opinion%2011-01%20--%20Software%20as%20a%20Service%20-%20Cloud%20Computing.pdf. As suggested by the Iowa opinion, lawyers must be able to access the lawyer's own information without limit, others should not be able to access the information, but lawyers must be able to provide limited access to third parties to specific information, yet must be able to restrict their access to only that information. *Id.*

Iowa Ethics Opinion 11-01 also recommends considering the reputation of the service provider to be used, its location, its user agreement and whether it chooses the law or forum in which any dispute will be decided, whether it limits the service provider's liability, whether the service provider retains the information in the event the lawyer terminates the relationship with the service provider, what access the lawyer has to the data on termination of the relationship with the service provider, and whether the agreement creates 'any proprietary or user rights' over the data the lawyer stores with the service provider. *Id.* It also suggests that the lawyer determine whether the information is password protected, whether the information is encrypted, and whether the lawyer will have the ability to further encrypt the information if additional security measures are required because of the special nature of a particular matter or piece of information. *Id.* It further suggests that the lawyer consider whether the information stored via cloud computing is also stored elsewhere by the lawyer in the event the lawyer cannot access the information via 'the cloud.'" *Id.*

90. *Terms of Service*, GOOGLE, *supra* note 86.

91. *Services Agreement*, MICROSOFT, http://windows.microsoft.com/en-us/windows-live/microsoft-services-agreement (last visited June 5, 2014).

92. *Terms of Service,* DROPBOX, https://www.dropbox.com/terms (last visited June 5, 2014).

93. *Id.*

Google's terms contain a similar limitation: "The rights you grant in this license are for the limited purpose of operating, promoting, and improving our Services, and to develop new ones."[94] Microsoft's terms also provide that uploaded content "may be used, modified, adapted, saved, reproduced, distributed, and displayed to the extent necessary to protect you and to provide, protect and improve Microsoft products and services."[95] As one observer put it, "That's pretty much exactly the same set of rights Google is asking for, with the same limitations. The reasons are the same, too: Microsoft needs to be able to move and change your content at will in order to run its services."[96] However, intellectual property ownership and data content rights issues are not the only provisions in the terms of use that should make even the most casual cloud user pause. Among the terms of use for Google, DropBox, Microsoft and Go Daddy, for example, each have very circumscribed "limitation of liability" provisions. When coupled with the preclusion from bringing claims for consequential damages, lost profits, incidental, special or punitive damages, these provisions have the effect of severely limiting the scope and breadth of a subscriber's ability to recover anything close to the actual damages that would be suffered in the case of a major data security breach.[97]

In the case of Google and Go Daddy, the limitation of liability provision caps damages to the amount of fees paid by the subscriber in connection with the service.[98] Other cloud providers place even greater limits to the monetary scope of recovery under their terms of use. Dropbox, for example, limits liability on "all claims relating to the service" to "the greater of $20 or the amounts paid by you to Dropbox for the past twelve months of the services in question."[99] Given that Dropbox's current pricing starts at "zero" for the basic cloud storage package and goes up to $15 per month for a business account offering unlimited storage,

---

94. *Terms of Service*, GOOGLE, *supra* note 86.

95. *Services Agreement*, MICROSOFT, *supra* note 91.

96. Nilay Patel, *Is Google Drive worse for privacy than iCloud, Skydrive, and Dropbox?*, THE VERGE (Apr. 25, 2012, 11:09 AM), http://www.theverge.com/2012/4/25/2973849/google-drive-terms-privacy-data-skydrive-dropbox-icloud. "[I]t's expansive language, but it's clear that Google's after the ability to run its services and sell targeted ads, not dig around in your Drive folders." *Id.*

97. *Terms of Service*, GOOGLE, *supra* note 86; *Terms of Service*, DROPBOX, *supra* note 92; *Services Agreement*, MICROSOFT, *supra* note 91;

Agreement, GO DADDY, https://cart.m.godaddy.com/cart/agreement.aspx?refurl=http%253a%252f%252fwww.godaddymobile.com%252fproducts%252fproducts.aspx&agreementType=WST_EULA&ci=19140 (last visited June 5, 2014).

98. *Terms of Service*, GOOGLE, *supra* note 86; *Agreement*, GO DADDY, *supra* note 97.

99. *Terms of Service*, DROPBOX, *supra* note 92.

the net result is a limitation on damages on a claim (on the low-end) from $20 to a high of $180 in the case of a business account.[100] And Microsoft is stingier still, limiting liability to direct damages "up to an amount equal to your service fee for one month."[101]

Other material terms contained in these terms of use, such as warranties and indemnification, do not provide any better alternatives from the subscriber's perspective. Indeed, such provisions merely serve to further tilt the already asymmetric legal and financial position in favor of the cloud provider. For example, the Google, Microsoft, Dropbox, and Go Daddy's terms of use, all clearly state that their cloud services are provided "as is" and expressly disclaim basic standard warranties, such the express and implied warranties of merchantability and fitness for a particular purpose.[102] In the case of Go Daddy, its terms of use actually require the user to broadly indemnify Go Daddy for any claims arising from "your use of and access to [the Go Daddy site] or the [s]ervices" on the site.[103] While such an indemnification provision did not exist in the other terms of use that were reviewed, other provisions such as mandatory arbitration and class action waivers (appearing in both the Dropbox's and Microsoft's terms of use) serve to limit the avenues of recourse of an aggrieved party.[104]

If unfavorable terms like these make the casual cloud user uneasy about uploading ordinary, every-day content, shouldn't they make an attorney, subject to the highest ethical obligations, and liable both financially and professionally for running afoul of them, turn and run the other direction as fast as her lawyer legs will carry her? More generally, if an attorney, for any of the reasons discussed above, decides to venture into the cloud, how should she read, and react to, providers' terms of service to avoid running afoul of the Model Rules?

If Comment 8's admonition to "keep abreast of . . . the benefits and risks associated with relevant technology" means that an attorney remain aware of changes to their own cloud service providers' terms of service, does it also require that an attorney "keep abreast" of broader terms of service trends in the cloud computing industry? And reading

---

100. *See Dropbox Upgrade*, DROPBOX, https://www.dropbox.com/plans (last visited June 5, 2014); *Terms of Service*, DROPBOX, *supra* note 92.

101. *Services Agreement*, MICROSOFT, *supra* note 91.

102. *Terms of Service*, GOOGLE, *supra* note 86; *Terms of Service*, DROPBOX, *supra* note 92; *Services Agreement*, MICROSOFT, *supra* note 91; *Agreement*, GO DADDY, *supra* note 97.

103. *Universal Terms of Service*: *Section 16 (Indemnity)*, GO DADDY, http://www.godaddy.com/legal-agreements.aspx (last visited June 5, 2014).

104. *Terms of Service,* DROPBOX, *supra* note 92; *Services Agreement*, MICROSOFT, *supra* note 91.

terms of use or even keeping abreast of broader trends regarding terms of use is one thing, taking some definitive action or step with respect to such terms or developments is quite another. Most, if not all, law firms will be close to powerless to change the terms of service offered by a company like Google or Microsoft.[105] To the extent any proactive measures are taken, attorneys will be shopping for, rather than negotiating for, the most favorable terms. If two cloud service providers, of similar size and prestige, offer similar services at comparable price points (and therefore offer, to use the language in Comment 8, similar "benefits") is an attorney in violation of Rule 1.1 by employing one with the less favorable terms of use provision, and thereby increasing the "risks associated with relevant technology"?[106]

As discussed above, Comment 3 to Rule 5.3 says that the extent of a lawyer's obligation will depend on, in addition to "the terms of any arrangement concerning the protection of client information," "the education, experience and reputation of the non-lawyer." This suggests an inverse relationship between the attorney's responsibility and the expertise of the cloud services provider. Would an attorney be foolish to enlist cloud services from a new, lesser-known startup company? Paradoxically, the very companies with whom an attorney will have little or no leverage to negotiate favorable terms of services are precisely those providers with whom a responsible attorney will be wise, from a security perspective, to contract. In complying with the Model Rules, what recourse does this leave to the responsible attorney, other than to take the leap of faith that every other average Internet user takes when she uploads her most precious photographs, sensitive financial information, or her screenplay to the cloud?

Indeed, the leap of faith is, because of market forces, perhaps no greater than the one previously required to entrust physical boxes of documents to a storage company or when photocopying client docu-

---

105. Dave Smith, *The Google Drive Price Cut Changes The Game For Personal Cloud Storage*, READWRITE (Mar. 17, 2014), http://readwrite.com/2014/03/17/google-drive-pricing-plans-drop-cloud-rivals-breakdown#awes m=~oz4RRacaOTWF4s. This powerlessness derives not merely from a firm's size relative to a cloud service provider, but from the relative cheapness of cloud storage space. Google, for example, offers 10 terabytes of space, its largest offering, on Google Drive for $100 a month. *Id*. Even if a law firm needed 10 terabytes, no single user, even a powerful law firm, is wielding a very long lever in negotiations with Google at that price. *Id.*; *see also* Leslie Johnston, *How many Libraries of Congress does it take?*, THE SIGNAL (Mar. 23, 2012), http://blogs.loc.gov/digitalpreservation/2012/03/how-many-libraries-of-congress-does-it-take/ ("…it is estimated that the entire collection of the Library of Congress including photos, sound recordings and movies might take 3,000 TB of storage. Assuming $100 each for 2 TB hard drives, the entire book collection of the Library of Congress could be stored on about $1500 worth of hard drives at today's prices.").

106. *See* MODEL RULES OF PROF'L CONDUCT R. 1.1cmt. 8 (2012).

ments was sent to an outside service.[107] As Nevada suggests, cloud computing can present:

> [T]he same risk [that] an employee of the warehouse, or some other person, will access and perhaps disclose the information without authorization. But neither the Model Rules nor the Supreme Court rules would prohibit the third-party storage arrangement altogether. Rather, they require the attorney to act reasonably and competently to protect the information from inadvertent and unauthorized access and disclosure.[108]

So why should attorneys keep abreast of changes to cloud security technology? Did the Model Rules require attorneys to do the same with warehouse security techniques? The market incentives for a cloud provider to maintain a reputation for security, not its terms of use, are the strongest assurance against the compromise of a client's information, and a vendor's reputation and track record, not the specific security systems it employs, are what an attorney should concern himself with.

Finally, as mentioned above, there is the issue of what is done with a client's information once representation has ended. New Hampshire advises that Rule 1.15 requires an attorney to ensure that a cloud service provider deletes the client's property from its servers:

> The data must be returned to the client and deleted from the cloud after representation is concluded or when the lawyer decides to no longer to preserve the file: in either case, the lawyer must know at all times where sensitive client information is stored, be it in the cloud or elsewhere.[109]

On this score, the terms of service of the most popular storage providers are more ambiguous. Microsoft, for example, says that:

> If you are canceling your services, the quickest means of eliminating your content on the services is to manually remove it from the various components of the services (for example, manually delete your email). However, please note that while content you have deleted or that is associated with a closed account may not be accessible to you, it may

---

107. Comment 3 to Model Rule 5.3 includes as examples of outside vendors, for whom lawyers have oversight responsibility, "sending client documents to a third party for printing." MODEL RULES OF PROF'L CONDUCT R. 5.3 cmt. 3 (2012); *see also* In Re Seroquel Prods. Liab. Litig., 244 F.R.D. 650 (M.D. Fla. 2007) (lawyers subject to sanctions from errors and omissions caused by their vendor).

108. State Bar of Nev. Comm. on Ethics and Prof'l Responsibility, Formal Op. 33 (2006), *available at* http://ftp.documation.com/references/ABA10a/PDfs/3_12.pdf.

109. N.H. Bar Ass'n Ethics Comm. Op. 2012-13/4 (2013), *available at* http://www.nhbar.org/legal-links/Ethics-Opinion-2012-13_04.asp.

still remain on our systems for a period of time.[110]

While not all states have addressed this issue, it may be necessary for an attorney, at a minimum, to inform the client of the possibility that content may linger on the cloud provider's servers for a period of time after representation has ended.

V. A SIMPLER APPROACH

The ethics opinions promulgated by various state bar associations put a big responsibility on the attorney. He is not asked merely to "keep abreast of…the benefits and risks associated with relevant technology," as prescribed by the Model Rules, but in some states also to keep abreast of why, at any given point in time, one cloud vendor is more secure than the others, and how vendors are evolving to face security threats.[111] The ethics opinions discussed above also overestimate an attorney's leverage to negotiate favorable terms with a cloud service provider. Overall, the opinions betray unfamiliarity, and perhaps a reflexive discomfort, with cloud computing in general, one which is out of step with the general public's wide and continuing integration of cloud computing into everyday life.[112]

---

110. *Services Agreement*, MICROSOFT, *supra* note 91; Google's terms state, even more ambiguously, that "[t]his license continues even if you stop using our Services (for example, for a business listing you have added to Google Maps). Some Services may offer you ways to access and remove content that has been provided to that Service." *See Terms of Service*, GOOGLE, *supra* note 86; Dropbox's terms are the clearest:

> We'll retain information you store on our Services for as long as we need it to provide you the Services. If you delete your account, we'll also delete this information. But please note: (1) there might be some latency in deleting this information from our servers and back-up storage; and (2) we may retain this information if necessary to comply with our legal obligations, resolve disputes, or enforce our agreements.

Terms of Service, DROPBOX, *supra* note 92

111. *See*, *e.g.*, Or. State Bar, Formal Op. 2011-188 (2011), available at http://www.osbar.org/_docs/ethics/2011-188.pdf ("Lawyer may be required to reevaluate the protective measures used by the third-party vendor to safeguard the client materials."); Fla. Bar Ethics Op. 12-3 (2013), *available at* https://www.floridabar.org/__85256AA9005B9F25.nsf/0/9DA5423ABE78318685257B0100535ADD?OpenDocument (requiring a lawyer to "[i]nvestigat[e] the online data storage provider's security measures, policies, recoverability methods, and other procedures to determine if they are adequate under the circumstances").

112. For a glimpse of cloud computing's future, *see, e.g.*, David Politis, *Growing Up Google: How Cloud Computing Is Changing a Generation*, MASHABLE, (Apr. 30, 2012), http://mashable.com/2012/04/30/generation-growing-up-google/ ("Nearly half of Gmail's overall user base is under 25, a statistic mirrored by the student bodies of American colleges and universities. Of the nation's top 100 universities 66 have already gone Google. According to Northwestern, one of the first universities to make this move, students actually requested that the school implement the platform. A majority of students were al-

Rather than requiring an attorney to secure unrealistic guarantees from vendors, or saddling her with an exhaustive list of factors to be considered before taking advantage of cloud computing, the following measures provide a more common sense approach to the ethics of cloud computing, and allow an attorney to benefit from, without being burdened or distracted by, the technology.

A. INFORMED CONSENT

Although Model Rule 1.6 contemplates securing a client's consent to reveal information to a third party—"[a] lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent"—the various states that have taken up the problem of cloud computing proceed on the assumption that "the disclosure [to a vendor] is impliedly authorized in order to carry out the representation" and that, rather than seeking consent, the attorney will use "reasonable efforts" to ensure confidentiality.[113]

Two states contemplate consent as an additional measure when the client's information is particularly sensitive. California says that "[i]f the information is of a highly sensitive nature and there is a risk of disclosure when using a particular technology, the attorney should consider alternatives unless the client provides informed consent,"[114] and New Hampshire advises that "where highly sensitive data is involved, it may become necessary to inform the client of the lawyer's use of cloud computing and to obtain the client's informed consent."[115] Similarly, Pennsylvania adds that "[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."[116]

But the opinions do not prescribe that an attorney be upfront with a client about cloud computing. Presumably, there is concern that a cli-

---

ready forwarding email to Gmail.").

113. *See* Cal. State Bar, Formal Op. 2010-179 (2010), *available at* http://ethics.calbar.ca.gov/LinkClick.aspx?fileticket= wmqECiHp7h4%3D&tabid=837 ("There is a distinction between actually disclosing confidential information to a third party for purposes ancillary to the representation, on the one hand, and using appropriately secure technology provided by a third party as a method of communicating with the client or researching a client's matter, on the other hand.").

114. *Id.*

115. N.H. Bar Ass'n Ethics Comm. Op. 2012-13/4 (2013), *available at* http://www.nhbar.org/legal-links/Ethics-Opinion-2012-13_04.asp.

116. Pa. Bar Ass'n on Legal Ethics and Prof'l Responsibility Op. 2011-200 (2011), *available at* http://www.slaw.ca/wp-content/uploads/2011/11/2011-200-Cloud-Computing.pdf.

ent may balk at a cloud computing provision in a fee agreement. But is this concern justified? As mentioned above, lawyers have been slower than professionals in other industries to adopt cloud computing.[117]

The model rules explain that informed consent "denotes the agreement by a person to a proposed course of conduct after the lawyer has communicated adequate information and explanation about the material risks of and reasonably available alternatives to the proposed course of conduct."[118] California advises that, when an attorney is seeking consent to store especially sensitive information in the cloud:

> [T]he attorney should fully advise the client about the nature of the information to be transmitted with the technology, the purpose of the transmission and use of the information, the benefits and detriments that may result from transmission (both legal and non-legal), and any other facts that may be important to the client's decision. (Los Angeles County Bar Assn. Formal Opn. No. 456 (1989).) It is particularly important for an attorney to discuss the risks and potential harmful consequences of using the technology when seeking informed consent.[119]

While the incorporation of such concepts with specific language in an engagement letter/fee agreement would not relieve an attorney from their obligations under the model rules and applicable state bars in which they are licensed and therefore much of the burden of teaching herself the ins and outs of cloud security would remain, there is no question such language would be the only prudent approach for an attorney seeking to comply with the applicable and limiting risk with their clients.[120]

B. SPECIALTY VENDORS

There is also an emerging group of cloud vendors marketed to users who want a higher level of security. These providers are reasonably inexpensive and boast security measures that are not employed by the

---

117. Black, *supra* note 8.

118. MODEL RULES OF PROF'L CONDUCT R. 1.0(e) (2012).

119. Cal. State Bar, Formal Op. 2010-179 (2010), *available at* http://ethics.calbar.ca.gov/LinkClick.aspx?fileticket= wmqECiHp7h4%3D&tabid=837.

120. Of course the mere execution of such an agreement alone would, in the event of a reach, be insufficient to discharge the lawyer of her duties, since it would be essential also to ensure that there was compliance with all applicable rules, regulations and laws, including the data breach notification laws required now required in 46 of the 50 states. *See, State Data Security Breach Notification Laws*, MINTZ LEVIN (Dec. 1, 2013), *available at* http://www.mintz.com/newsletter/2007/PrivSec-DataBreachLaws-02-07/state_data_breach_matrix.pdf ("As of December 1, 2013, Alabama, Kentucky, New Mexico and South Dakota have no laws related to security breach notification.").

more popular vendors discussed above.[121] Wuala, for example, provides for files to be encrypted by the attorney before they're uploaded to the providers' servers, which means that no one, not even Wuala, can access the client's files.[122] Wuala also has a "zero-knowledge password policy," by which the password can only be known by the user. A vendor with this type of password policy cannot, even at the request of law enforcement, access the uploaded files.[123] Cloud vendor Tresorit, like Wuala, provides for client-side encryption of files and does not know users' passwords.[124] Unlike Wuala, Tresorit allows for these heightened security measures to be applied selectively to different files and folders uploaded to the cloud, useful if an attorney wants heightened protection for a subset particularly sensitive client data.[125] Another cloud storage provider, McAfee, even offers some security measures which may, to most attorneys, seem like overkill, but nevertheless in certain matters such as the early stages of a top-secret Merger & Acquisition or, in the case of highly sensitive litigation involving say, trade secret materials that may be subject to a Protective Order, with an "Attorney-Eyes Only" designation, may be perfectly justifiable. Specifically, McAfee's Personal Locker, a phone-based app, utilizes voice, biometric data (face recognition), as well as a PIN number before allowing access to files.[126] Although McAfee's service is not designed as an all-purpose cloud service, it would make the attorney's remote access from a phone more secure, a problem at least one state bar association considers expressly.[127]

Of course, knowing precisely to what degree the security measures

---

121. *See* Sarah J. Purewal, *Loaded and locked: 3 seriously secure cloud storage services*, PCWORLD (Mar. 6, 2014, 3:00 AM), *available at* http://www.pcworld.com/article/2105100/loaded-and-locked-3-seriously-secure-cloud-storage-services.html.

122. For a complete description of security measures visit the Wuala website. Security, WUALA, http://www.wuala.com/en/learn/technology (last visited June 11, 2014). ("Wuala features best-in-its class privacy and data security. All files are encrypted on your computer before being transferred to the cloud. Your password never leaves your computer, so no unauthorized user, not even LaCie employees, could ever access your data.").

123. *Id.*

124. Purewal, *supra* note 121.

125. *See Features Designed to Enchance Productivity and Champion your Data's Security*, TRESORIT, https://tresorit.com/features (last visited June 11, 2014).

126. Purewal, *supra* note 121.

127. *See* Mass. Bar Ass'n Comm. on Prof'l Ethics Op. 12-03 (2012), *available at* http://www.massbar.org/publications/ethics-opinions/2010-2019/2012/opinion-12-03 (addressing a hypothetical in which "[a] lawyer ("Lawyer") wishes to store and synchronize the electronic work files that he creates in the course of his law practice across multiple computers and devices (e.g., smartphones, iPads, etc.) so that he can access them remotely.").

of these specialty vendors protects a client's data over and above their competitors may, as suggested above, be outside a lawyer's realm of expertise. This is where certifications conducted by independent third parties who can, based on an objective set of criteria, assess and measure the robustness of cloud security of service providers could be particularly noteworthy. If the standards are met, the cloud service is certified and can then widely publicize that fact. For example, Truste.com, which historically has provided its "privacy seal" to those enterprises that have met Truste.com's pre-determined levels of privacy compliance, now also offers certification services seals for companies providing cloud services.[128] An attorney can at least rely to some degree on the expertise of these independent third party certifications. While reliance on such certifications alone would be ill-advised for an attorney striving to comply with all the applicable ethical obligations and rules of professional responsibility, it would nevertheless supply some justification that some basic standards were met. At a minimum, marketing research demonstrates the importance of these privacy seals and certifications in building trust and confidence.[129]

In short, the use of a security-focused cloud provider may provide a way for an attorney to utilize the cloud with confidence, and without having to negotiate special terms with a vendor or become an expert in cloud technology.

C. CYBER INSURANCE

Finally, for an attorney who wants an extra layer of protection against the risks of cloud computing, there are now insurance policies available that are specifically tailored for cyber security. Although this segment of the insurance industry is still in its infancy, there are al-

---

128. *Cloud Privacy Certification*, TRUSTE, http://www.truste.com/products-and-services/enterprise-privacy/TRUSTed-cloud (last visited June 5, 2014).

129. Christine Yee, *Toward an Integrated Understanding of Online Trust* (July 9, 2013) (Ph.D. electronic dissertation, Florida State Univ.), *available at* http://diginole.lib.fsu.edu/cgi/viewcontent.cgi?article=7671&context=etd&sei-redir=1&referer=http%3A%2F%2Fwww.google.com%2Furl%3Fsa%3Dt%26rct%3Dj%26q%3Dtowards%2520a%2520model%2520for%2520enhancing%2520consumer%2520trust%2520in%2520an%2520online%2520environment%26source%3Dweb%26cd%3D16%26ved%3D0CFEQFjAFOAo%26url%3Dhttp%253A%252F%252Fdiginole.lib.fsu.edu%252Fcgi%252Fviewcontent.cgi%253Farticle%253D7671%2526context%253Detd%26ei%3D6MNIU7boDoThyQHanoHgCg%26usg%3DAFQjCNEJVmmMETXu-hE55J5ED8Q5ix2GoQ%26sig2%3DtvL4-bsIcvOx6M3xhUPFIw%26bvm%3Dbv.64542518%2Cd.aWc#search=%22towards%20model%20enhancing%20consumer%20trust%20an%20online%20environment%22.

ready estimated to be more than 60 companies that insure against "exposure, loss, or misuse of data, whether through a targeted hacker attack or the simple loss of a smartphone," and offer coverage for "liability for the disclosure of third-party data, data recreation or recovery, and expenses for forensic work to uncover how the breach happened, what was lost, and whether or not it was put to use."[130]

As the ABA notes, traditional insurance provides insufficient coverage in the event of a cyber-attack, but "cyber liability policies can address issues ranging from privacy breach notification and crisis management to regulatory defense and civil penalties to liability resulting from a privacy breach."[131] Some policies even provide for public relations assistance in the event of a breach. Several commentators have advocated undertaking a coverage analysis of current policies.[132] Such an analysis might ask, for example, whether the policy specifically covers "intangible information assets" or the wrongful collection or dissemination of data, or whether "the policy cover[s] claims against the firm[s] that are due to a third party IT or security vendor."[133] In sum, even though many law firms still have not yet widely adopted cyber liability coverage, the trend is that they will continue to do so in greater numbers.[134] To the extent this occurs, cyber liability policies can only assist in reducing risk and liability to attorneys who utilize cloud services.

VI. CONCLUSION

So is it safe for an attorney to enter the cloud? The various state bar associations that have so far addressed the question have all answered "yes," but left the lawyer with onerous and bewildering obligations to "keep abreast," not merely of "the benefits and risks associated with relevant technology," as Comment 8 to Model Rule 1.1 suggests,

---

130. Andrew Strickler, *Cyber Insurance Options Grow for Law Firms*, LAW360 (Jan. 24, 2014 8:03 PM), *available at* http://www.law360.com/articles/503623/cyberinsurance-options-grow-for-law-firms.

131. *Protect your firm: Invest in cyber liability insurance*, ABA, (July, 2013), http://www.americanbar.org/newsletter/publications/youraba/201307article04.html.

132. *Id.*

133. *See* Kevin P. Kalinich, *Network Risk Insurance 2012: Privacy & Security Exposures and Solutions for Law Firms*, LAW PRACTICE TODAY (Mar. 2012), http://www.americanbar.org/content/dam/aba/publications/law_practice_today/network-risk-insurance-privacy-security-exposures-and-solutions-for-law-firms.authcheckdam.pdf.

134. *Experts Warn to Protect Themselves Against Cyberattacks*, ABA NEWS, (Feb. 18, 2014, 11:18 AM), http://www.americanbar.org/news/abanews/aba-news-archives/2014/02/experts_warn_lawfir.html.

but of the particulars of a cloud vendor's security measures.[135] Some of the opinions discussed above also significantly overstate an attorney's ability to negotiate special protections from cloud vendors, and ignore the reality that large, well-known and reputable vendors, whom the attorney might be well-advised to select, will probably be the least likely to alter their terms. Overall, the attitude among the state bar associations appears to be animated by an unjustified fear. Nevada notes that:

> [T]he risk, from an ethical consideration, is that a rogue employee of the third party agency, or a 'hacker' who gains access through the third party's server or network, will access and perhaps disclose the information without authorization. In terms of the client's confidence, *this is no different in kind or quality than the risk that a rogue employee of the attorney, or for that matter a burglar, will gain unauthorized access to his confidential paper files.* The question in either case is whether the attorney acted reasonably and competently to protect the confidential information.[136]

The analogy to paper files, which cannot be disseminated or replicated with the rapidity of electronic files, is not perfect. However, rather than becoming a technology expert, an attorney may discharge her ethical duties by disclosing and explaining to her clients the use of cloud computing, employing an especially secure cloud vendor, procuring cyber insurance, or some combination of these three. These simple measures would, unlike the sometimes impractical and unrealistic measures suggested by the various states in their opinions and rules, allow an attorney to take advantage of cloud computing easily and with a clear conscience. That is a good thing for clients. As New Jersey, explains, "[t]he polestar is the obligation of the lawyer to engage in the representation competently, and to communicate adequately with the client and others. To the extent that new technology now enhances the ability to fulfill those obligations, it is a welcome development."[137]

---

135. *See* MODEL RULES OF PROF'L CONDUCT R. 1.1cmt. 8 (2012).

136. State Bar of Nev. Comm. on Ethics and Prof'l Responsibility, Formal Op. 33 (2006), *available at* http://ftp.documation.com/references/ABA10a/PDfs/3_12.pdf (emphasis added).

137. N.J. Advisory Comm. on Prof'l Ethics Op. 701 (2006), *available at* http://www.judiciary.state.nj.us/notices/ ethics/ACPE_Opinion701_ElectronicStorage_12022005.pdf.