

GOING GOOGLE: YOUR PRACTICE, THE CLOUD, AND THE ABA COMMISSION ON ETHICS 20/20

Shellie Stephens*

TABLE OF CONTENTS

I.	Introduction.....	237
II.	Cloud Computing, or, “Screens Connected to the Web”	238
III.	Discussion.....	241
A.	The Standard, Model Rule 1.6, and its Inherent Uncertainty.....	241
B.	State of Interpretation	243
C.	Comments From the Bar, Judiciary, and Public	245
IV.	Recommendation and Conclusion	246

I. INTRODUCTION

In August 2009, American Bar Association President Carolyn B. Lamm created the Commission on Ethics 20/20¹ to consider whether the Model Rules of Professional Conduct (MRPC)² adequately address the challenges of a twenty-first century law practice.³ In its first meeting, the Commission identified critical issues raised by emerging technology. These issues included concerns regarding the privacy and security of client confidential data stored online on third-party servers and the acceptable level of data access by providers.⁴ The Commission requested comments and recommendations from

* J.D. *cum laude*, University of Illinois College of Law, 2011.

1. ABA COMM’N ON ETHICS 20/20, PRELIMINARY ISSUES OUTLINE (Nov. 19, 2009), *available at* <http://www.americanbar.org/content/dam/aba/migrated/ethics2020/outline.authcheckdam.pdf>.

2. Specifically Model Rule 1.6, Confidentiality of Information, for the purposes of this Recent Development: “(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” MODEL RULES OF PROFESSIONAL CONDUCT R. 1.6 (2002).

3. *Message from Commission on Ethics 20/20 Co-Chairs Jamie S. Gorelick and Michael Traynor*, AM. BAR ASS’N, http://www.americanbar.org/groups/professional_responsibility/aba_commission_on_ethics_20_20/about_us/message_from_the_co_chairs.html (last visited Mar. 27, 2011).

4. *Id.* The Commission will conduct a plenary review and assessment of the Model Rules “in the context of rapid societal change with regard to globalization and technological innovation.” Lance J. Rogers, *Ethics 20/20 Commission Invites Comments On Issues Raised by Growing Use of Internet*, 26 LAW MANUAL ON PROF. CONDUCT 586, 586 (2010), *available at* http://www.americanbar.org/content/dam/aba/migrated/ethics2020/aba_bna.authcheckdam.pdf. The Commission’s first meeting was held September 24–25, 2009.

the bar, judiciary, and public on whether formal comment or guidance from the ABA was needed regarding the technological issues presented, and if so, in what form.⁵ The options under consideration included a white paper, an online resource, and proposed amendments to the Model Rules.⁶ The comments received were overwhelmingly in favor of practical guidance in some form of an ABA online guide, which would identify best practices and educate practitioners on the benefits and risks of emerging technologies.⁷

This Recent Development will examine one part of the ABA—greater bar discussion, the professional obligation to take reasonable steps to protect electronically stored client confidential data from inadvertent disclosure or unauthorized access. Part II provides a brief introduction to the related computing concepts. Part III focuses on the relevant Model Rule, Rule 1.6 and comment seventeen thereto, and the current state of interpretation. Part IV will note and adopt several of the recommendations received by the Commission, which advocate the development of a publicly available and continually updated online technology portal. Additionally, revisions to Model Rule 1.6, comment seventeen, will be proposed.

II. CLOUD COMPUTING, OR, “SCREENS CONNECTED TO THE WEB”⁸

Data storage and access is occurring increasingly online, and sometimes exclusively online, as society moves its data to online service providers and utilizes free or inexpensive online software applications that provide web-native⁹ access and management.¹⁰ Even though the amount of information we are accessing and accumulating is increasing,¹¹ there is less need for local storage or personal computers with cavernous hard drives. The trend away from identifying data storage and access with local, on-site storage is popularly referred to as migration to the “cloud.”¹² In response to increased demand for

5. Rogers, *supra* note 4, at 586.

6. *Id.* Specifically, the Commission suggested possible amendments to “Model Rule 1.1 (competence), Model Rule 1.6 (confidentiality), and Model Rule 1.15 (safeguarding client property).” *Id.*

7. ABA Comm’n on Ethics 20/20, Comments, Technology Working Group Issues Papers (Jan. 24, 2011), http://www.americanbar.org/content/dam/aba/migrated/2011_build/ethics_2020/20110124.pdf [hereinafter Technology Working Group Issues Papers].

8. “I predict most people will do their work on ‘screens connected to the web.’ There won’t be any sort of ‘computer’ anymore.” Janna Anderson, *The Future of Cloud Computing*, PEW RESEARCH CENTER, at 9 (Jun. 2010), http://pewinternet.org/~media/Files/Reports/2010/PIP_Future_of_the_Internet_cloud_computing.pdf (quoting Davis Fields, Product Manager, Nokia).

9. At the time of this writing a definition of “web-native” was not found. Here, “web-native” will refer to a program that was designed and built specifically for the Internet and to run via a web browser such as Microsoft Internet Explorer, Mozilla Firefox, or Google Chrome.

10. John B. Horrigan, *Cloud Computing Gains in Currency: Online Americans Increasingly Access Data and Applications Stored in Cyberspace*, PEW RESEARCH CENTER (Sept. 12, 2008), <http://pewresearch.org/pubs/948/cloud-computing-gains-in-currency>.

11. Seventy-four percent of Americans are online; greater than half of those users access the Internet over high-speed, broadband connections from home. LEE RAINIE, PEW RESEARCH CENTER, INTERNET, BROADBAND, AND CELL PHONE STATISTICS 2 (Jan. 5, 2010), available at http://pewinternet.org/~media/Files/Reports/2010/PIP_December09_update.pdf; AARON SMITH, PEW RESEARCH CENTER, HOME BROADBAND 2010 5 (Aug. 11, 2010), available at <http://pewinternet.org/~media/Files/Reports/2010/Home%20broadband%202010.pdf>.

12. For the purposes of this Recent Development, “cloud computing” will refer to the storage of user

cloud computing services, the computing industry is revolutionizing personal computing¹³ and software application offerings. Such changes will impact future hardware and software options available to the legal professional and almost certainly decrease the costs of information management.

Cloud computing providers offer free or low-cost alternatives to expensive applications and storage on a user's personal computer.¹⁴ The providers often offer their resources free of charge in exchange for access to and subsequent monetization of user data. Typically, the access includes the electronic scanning of user data for content¹⁵ that can then be used to serve linked, targeted advertisements to the user.¹⁶ Paid online resources are available and frequently operate on the principle of "scalability,"¹⁷ or the ability to add greater values with minimal effort and expense.¹⁸ In addition to these significant cost savings, cloud computing offers users cross-platform access,¹⁹ elegant collaboration and synchronization tools,²⁰ and redundancy of data which potentially provides additional data security.²¹ These benefits place

data online on third-party servers and software applications which are executed in a web browser. Citing the growing demand for cloud computing, Dave Armstrong, the head of product and marketing for Google Enterprise, stated, "There's a clear direction . . . away from people thinking, 'This is my PC, this is my hard drive,' to 'This is how I interact with information, this is how I interact with the web.'" David Smith, *Google Plans to Make PCs History*, THE OBSERVER, Jan. 25, 2009, <http://www.guardian.co.uk/technology/2009/jan/25/google-drive-gdrive-internet>.

13. For instance, the industry is now promoting personal computers with little or no internal storage that are little more than "portals" to the Internet, that store a user's files and even the operating system itself, on remote servers. The computer itself is "software" rather than "hardware" as it is now conceived. *Id.*

14. See, e.g., *More Google Products*, GOOGLE, <http://www.google.com/intl/en/options> (last visited Mar. 8, 2011) (displaying various free web-based applications).

15. See, e.g., *More on Gmail and Privacy: Scanning Email Content*, GMAIL, http://mail.google.com/mail/help/about_privacy.html#scanning_email (last visited Mar. 8, 2011) (explaining Google's scanning of users' emails).

16. *More on Gmail and Privacy: Targeted Ads in Gmail*, GMAIL, http://mail.google.com/mail/help/about_privacy.html#targeted_ads (last visited Mar. 8, 2011).

17. *Scalable Definition*, THE LINUX INFORMATION PROJECT, <http://www.linfo.org/scalable.html> (last visited Mar. 8, 2011).

18. For example, adding more storage as needed or more users in the case of application access. Amazon's S3, Simple Storage Service, uses a "pay only for what you use" pricing structure. The prices vary from \$0.140 per gigabyte for the first fifty terabytes used per month to \$.055 per gigabyte when over 5000 terabytes are used monthly. *Amazon Simple Storage Service (Amazon S3)*, AMAZON.COM, <http://aws.amazon.com/s3/#pricing> (last visited Mar. 8, 2011).

19. Access to traditional software was often limited by hardware compatibility, operating system, and licensing. Because cloud computing solutions are web-based, they are generally compatible across platforms (Mac, PC, Linux, etc.) and browsers (Internet Explorer, Firefox, Chrome, Safari, etc.).

20. Collaborative tools, such as Google Docs, allow multiple users to simultaneously access a document and the edits of one user are automatically and instantaneously reflected on other users' screen. *Simultaneous Editing and Viewing*, GOOGLE DOCS, <http://docs.google.com/support/bin/answer.py?hl=en&answer=44680> (last visited Mar. 8, 2011). For the power user, the concepts of synchronization and collaboration are intertwined. Data that is accessed from more than one computer typically is read-only. In that instance, the data is not changed in any significant way. However, if the data is edited, synchronizing the changes so that the changes are simultaneously reflected in the document and apparent, viewable, and re-editable from any access-point is a huge benefit, providing the user with access to the latest version of the document no matter where it is accessed. Dropbox is an especially popular synchronization tool. G.F., *Dropbox: There's Room Yet in the Cloud*, THE ECONOMIST BABBAGE BLOG (Aug. 4, 2010, 5:21 PM), <http://www.economist.com/blogs/babbage/2010/08/dropbox>.

21. While online storage of client data presents serious security concerns, an argument can be made that online data storage is safer than local storage—the most common cause of data breaches is lost or stolen memory sticks and laptops. Sixty-six percent of USB sticks, a portable data device, are lost and of those, sixty

the latest technology within the reach of even the smallest law firm or solo practitioner.²²

Google Applications are the Goliath of cloud computing providers.²³ Google's suite of online applications include: Gmail,²⁴ Google Calendar,²⁵ Google Documents,²⁶ and Google Photos.²⁷ Google Documents includes Google Spreadsheets and Google Presentations—two products that duplicate the functionality of Microsoft Office's Excel²⁸ and PowerPoint²⁹ applications at no cost for individual use.³⁰ Citing time and cost savings³¹ and increased worker productivity,³² millions of corporations³³ have migrated their company data to the cloud. Google calls this “going Google.”³⁴ Businesses and municipalities that have “gone Google” include the Cities of Los Angeles and Seattle, Motorola, and Salesforce.com.³⁵ On September 15, 2009, the United States Government announced it was moving to cloud-based IT services and

percent had commercial data stored on them. Warwick Ashford, *Cloud Computing More Secure Than Traditional IT, Says Google*, COMPUTERWEEKLY.COM (July 21, 2009, 5:04 PM), <http://www.computerweekly.com/Articles/2009/07/21/236982/cloud-computing-more-secure-than-traditional-it-says.htm>. However, the continued inadequate or nonexistent encryption technology offered by cloud computing providers requires serious contemplation by end users; unfortunately, the discussion is beyond the scope and page limits of this Recent Development. The author highly recommends Christopher Soghoian, *Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era*, 8 J. ON TELECOMM. & HIGH TECH. L. 359 (2010), for a thorough and easy-to-read understanding of the issues and potential market failure in this area.

22. Even though hard drive prices are relatively inexpensive, free backup of user data is a compelling reason to store data online, particularly given the ever-present specter of hard drive catastrophic failure. For reference, in 1995, a one-gigabyte hard drive retailed for \$625.00. *Cost of Hard Drive Space*, A LITTLE TECHNOLOGY SHOPPE, <http://ns1758.ca/winch/winchest.html> (last visited Mar. 8, 2011). Today, a one-terabyte external hard drive retails for \$79.99. *Omega Desktop External Drive*, AMAZON.COM, <http://www.amazon.com/lomega-Desktop-External-Drive-34836/dp/B0035J7XG2> (last visited Mar. 8, 2011).

23. GOOGLE APPS, <http://www.google.com/apps> (last visited Mar. 2, 2011).

24. GMAIL, <http://mail.google.com> (last visited Mar. 2, 2011).

25. GOOGLE CALENDAR, <http://www.google.com/calendar> (last visited Mar. 2, 2011).

26. GOOGLE DOCUMENTS, <http://docs.google.com> (last visited Mar. 2, 2011).

27. PICASA WEB ALBUMS, <http://picasaweb.google.com> (last visited Mar. 2, 2011).

28. *Excel*, MICROSOFT OFFICE, <http://office.microsoft.com/en-us/excel> (last visited Mar. 8, 2011).

29. *PowerPoint*, MICROSOFT OFFICE, <http://office.microsoft.com/en-us/powerpoint> (last visited Mar. 8, 2011).

30. Google offers Standard (free), Premier (business), Education (free), Government, and Non-Profit Organization editions of its popular offerings. GOOGLE APPS, <http://www.google.com/apps> (last visited Mar. 8, 2011).

31. In 2008, computer technology purchases, including hardware and software, accounted for half of all business capital spending. Steve Lohr, *Belt-Tightening, But No Collapse, is Forecast in Technology Spending*, N.Y. TIMES, Jan. 26, 2008, <http://www.nytimes.com/2008/01/26/technology/26spend.html>.

32. *Customer Stories*, GOOGLE APPS, <http://www.google.com/apps/intl/en/business/customers.html> (last visited Mar. 8, 2011). MWV (formerly MeadWestvaco), the 165-year old company behind Mead Five-Star notebooks, reports increased employee productivity since migrating their 12,000 “technology-enabled” employees to Google Apps. Colleen Horan, *MWV Has Gone Google*, OFFICIAL GOOGLE ENTERPRISE BLOG (Dec. 17, 2009, 9:18 AM), <http://googleenterprise.blogspot.com/2009/12/mwv-has-gone-google.html>.

33. Andy Berndt, “*Going Google*” with *Google Apps*, OFFICIAL GOOGLE ENTERPRISE BLOG (Aug. 3, 2009, 8:11 AM), <http://googleblog.blogspot.com/2009/08/going-google-with-google-apps.html> (“Over 1.75 million businesses, schools and organizations have gone Google—including Motorola, University of Notre Dame, the Mercy Corps and many more—and each day, 3,000 more organizations join them.”); Vivian Leung, *Over 2 Million Companies Have #goneGoogle Around the World*, OFFICIAL GOOGLE ENTERPRISE BLOG (Oct. 19, 2009, 3:10 PM), <http://googleenterprise.blogspot.com/2009/10/over-2-million-companies-have.html>.

34. Berndt, *supra* note 33.

35. *Businesses Share Their Stories*, GOOGLE APPS FOR BUSINESS, <http://www.google.com/apps/intl/en/business/customers.html> (last visited Mar. 8, 2011).

launched Apps.gov—an innovation expected to “save taxpayer dollars,” although it did not quantify the savings.³⁶ The government plans to rapidly expand its use of cloud computing and address security, privacy, and information issues as opportunities arise,³⁷ a luxury the government can afford.

Given the full-scale migration to the cloud and expectations that the most innovative application development work will be in the field of cloud computing,³⁸ it is foreseeable that future file management and litigation support tools will necessitate use of cloud resources by lawyers.³⁹ Because of the quantity of data lawyers are expected to process and store per case,⁴⁰ it would be burdensome to confine data storage and creation to in-house servers and software due to a misconception of the steps required under applicable rules of professional conduct to preserve client confidentiality. Therefore, Part III will examine the model rule and discuss the marked lack of uniformity in current interpretations of the steps required by state bar associations.

III. DISCUSSION

A. *The Standard, Model Rule 1.6, and its Inherent Uncertainty*

ABA Model Rule 1.6,⁴¹ which has a close analogue in every state, requires lawyers to maintain all information relating to the representation of a client in confidence, subject to very few exceptions⁴² and clarifying comments.⁴³ With respect to the transmittal of information that relates to client representation, the lawyer must take “reasonable precautions” to guard against inadvertent disclosure.⁴⁴ Special security measures are not required “if the method of communication affords a reasonable expectation of privacy,”⁴⁵

36. Vivek Kundra, *Streaming at 1:00: In the Cloud*, WHITE HOUSE BLOG (Sept. 15, 2009, 12:09 PM), <http://www.whitehouse.gov/blog/Streaming-at-100-In-the-Cloud>.

37. *Id.*

38. Press Release, Pew Internet & Am. Life Project, *Smartphones Expected to Drive Most Work from the Desktop to ‘the Cloud,’* available at <http://www.pewinternet.org/Press-Releases/2010/Cloud-Computing.aspx>.

39. Some programs that have enormous benefits for the legal professional are only available online such as AbsoluteProof® Data Integrity Protection, a digital service which provides proof of ownership and provides credibility to electronic records via an external time stamp. AbsoluteProof® Data Integrity Protection, SURETY, <http://www.surety.com/Offerings/AbsoluteProof.aspx> (last visited Mar. 8, 2011).

40. Virtually all cases today involve e-discovery on an unprecedented scale and many firms require software to handle the load. E-discovery is now in the gigabyte to terabyte realm and the transmittal and reception costs of such large amounts of data are not insignificant. Jerry F. Barbanel & Lee Curtis, *The Strategic Use of E-Discovery and High-Tech Experts in Complex Litigation, Regulatory and Compliance Matters*, THE METRO. CORP. COUNSEL, Jan. 2008, at 24, available at <http://www.metrocorpcounsel.com/pdf/2008/January/24.pdf>.

41. MODEL RULES OF PROF'L CONDUCT R. 1.6 (2002).

42. There are six exceptions to the rule. *Id.* R. 1.6(b).

43. There are eighteen comments to the rule. *Id.* R. 1.6 cmt. 1-18, available at http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_6_confidentiality_of_information/comment_on_rule_1_6.html.

44. MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. 17 (2002).

45. *Id.*

although some circumstances warrant special precautions.⁴⁶ To determine the necessary level of care, lawyers should consider the risk of harm, the likelihood of disclosure, and the extent to which the privacy of the communication is protected by either law or confidentiality agreement.⁴⁷ The responsibility for maintaining the confidentiality of client data is one of a duty of care,⁴⁸ which is not absolute or one of strict liability.⁴⁹

The language of comment seventeen to the Rule, ostensibly intended to clarify safe modes of transmission of client confidential data, is unfortunately now problematic: it refers to a method of communication which “affords a reasonable expectation of privacy.”⁵⁰ The phrase “reasonable expectation of privacy” is freight-laden and immediately calls to mind the complex history of Fourth Amendment jurisprudence.⁵¹ The answer of whether a reasonable expectation of privacy exists in a method of communication is not simple.⁵² While the ABA announced in 1999 that unencrypted email provides a reasonable expectation of privacy,⁵³ legal professionals may now be even more cautious given the uncharted terrain of constantly evolving technology and concomitant security standards. By tethering a lawyer’s ethical duties to an ever-shifting, fact-specific⁵⁴ legal standard, the Committee virtually guaranteed that every new trend or innovation in technology would rock the bar.⁵⁵

46. “A client may require the lawyer to use 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.” *Id.*

47. *Id.*

48. *Id.*

49. ABA Comm. on Ethics and Prof’l Responsibility, Formal Op. 99-413 (1999) (“It should be noted that a lawyer’s negligent use of any medium—including the telephone, mail and fax—may breach the duty of confidentiality.”).

50. MODEL RULES OF PROF’L CONDUCT R. 1.6 cmt. 17 (2002).

51. See generally *Katz v. United States*, 389 U.S. 347 (1967) (discussing whether a reasonable expectation of privacy existed for a conversation in a public phone booth).

52. The Supreme Court has propounded no single test. Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 503 (2007) (examining the four coexisting Supreme Court approaches to Fourth Amendment protection).

53. ABA Comm. on Ethics and Prof’l Responsibility, Formal Op. 99-413 (1999).

54. “Fourth Amendment jurisprudence is circular, confused, and often criticized because determining and balancing competing interests is vague and manipulable. As a jurist, the only practical way to proceed is through fact-intensive analysis of the individual case to try to find out what is a ‘reasonable expectation of privacy’ in the given factual context.” Eric Engle, *New Technologies and the Fourth Amendment*, HARV. J.L. & TECH. DIG., (Dec. 29, 2009), <http://jolt.law.harvard.edu/digest/privacy/digest-comment-new-technologies-and-the-fourth-amendment>.

55. This is precisely the situation in which the ABA finds itself when discussing reasonableness in the cloud—The *T. J. Hooper*, 60 F.2d 737 (2d Cir. 1932), has been invoked. The famous 1932 opinion held that tugboats, which did not carry radio receiving sets that could have provided the captain notification of changes in the weather, were unseaworthy, despite the fact that the receiving sets were not yet industry standard. *Id.* at 740. Judge Learned Hand stated that “there are precautions so imperative that even their universal disregard will not excuse their omission.” *Id.* Attorneys with *Hooperian* concerns may expend valuable time researching or worrying over which latest technological innovation is a judicial imperative they omit at their peril or will need to pay for an information technology consultant. The *T.J. Hooper* is wrongly invoked in this instance: to appropriately draw the analogy to lawyers and technology, to be “unseaworthy” or flagrantly dismissive of crucial client concerns, the lawyer would need to be wholly negligent—engaging in electronic transmission and reception of client information while ignoring technology in common usage such as password-protected email accounts or not password-protecting highly sensitive client data transmitted over the Internet. See N.J. Advisory Comm. on Prof’l Ethics, Op. 701 (2006), available at http://lawlibrary.rutgers.edu/ethics/acpe/acp701_1.html (stating that reasonable care is informed by the technology reasonably available at

The Supreme Court has not yet addressed the issue of whether a reasonable expectation of privacy exists in the contents of email. Presumably, any reasoning with regard to email privacy would carry over to cloud-based third-party provider transmission of client data necessary for storage and attorney-client access.⁵⁶ In 2007, the Sixth Circuit stated that a key component to maintaining a reasonable expectation of privacy is confirmation that files “provided” to third-party providers will not be monitored or audited.⁵⁷ Providers such as Google that electronically scan files to deliver targeted ads to the user could be implicated under such a standard. Third-party providers’ service agreements, specifying the level and type of provider access to the data, could then make a significant difference in the interpretation of the professional obligation. If the provider’s access to the data extinguishes any reasonable expectation of privacy, perhaps even to generate targeted advertisements, then use of the provider’s services may constitute an ethical breach.

B. State of Interpretation

Several state bar associations have addressed concerns related to third-party access to client data.⁵⁸ In each case, the use has been approved provided that sufficient precautions to ensure the safety and integrity of client data are

the time; reasonable care does not require the attorney to guarantee the data is invulnerable to unauthorized access, whether stored in the office or online).

56. The issue of whether e-mails, stored communications and communications-in-transit possess the same reasonable expectation of privacy as other correspondence is being discussed by legal scholars currently and is beyond the scope of this Recent Development. See Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005 (2010), for a proposed framework for the application of Fourth Amendment principles to cyberspace.

57. *Warshak v. United States*, 490 F.3d 455, 473 (6th Cir. 2007), *vacated and remanded on other grounds*.

58. See Ariz. Comm. on the Rules of Prof'l. Conduct, Op. 09-04 (2009), available at <http://www.myazbar.org/Ethics/opinionview.cfm?id=704> (allowing online storage of client data provided the lawyer takes reasonable precautions and conducts periodic review of the security measures in place); Mass. Bar Ass'n Comm. on Prof'l Ethics, Formal Op. 05-04 (2005), available at <http://www.massbar.org/publications/ethics-opinions/2000-2009/2005/opinion-05-04> (stating “reasonable efforts” must be taken to ensure that the conduct of any independent service provider is compatible with a lawyer’s professional obligations, including the obligation to protect confidential client information; the committee did not define reasonable efforts.); N.J. Advisory Comm. on Prof'l Ethics, Op. 701 (2006), available at http://lawlibrary.rutgers.edu/ethics/acpe/acp701_1.html (stating reasonable care must be taken with client data stored by a third-party service provider which must have an enforceable obligation to preserve client confidentiality and data security; available technology must be utilized to secure the data); N.Y. Comm. on Prof'l Ethics, Op. 842 (2010), available at http://www.nysba.org/AM/Template.cfm?Section=Ethics_Opinions&TEMPLATE=/CM/ContentDisplay.cfm&CONTENTID=42697 (allowing use of an outside online storage provider but requiring the lawyer to stay informed of technological advances and to monitor changing privilege laws); Vt. Bar Ass'n Comm. on Prof'l Responsibility, Advisory Ethics Op. 03-03 on Client Confidences (2003), available at <http://www.vtbar.org/Upload%20Files/WebPages/Attorney%20Resources/aeopinions/Advisory%20Ethics%20Opinions/Confidences%20of%20the%20Client/03-03.pdf> (stating contractors with access to client confidential data must understand and embrace the attorney’s duty of confidentiality; the attorney must ensure the contractor has adequate safeguards in place to protect client data). See also N.C. State Bar, Proposed 2010 Ethics Op. 7 (2010) (on file with author), <http://www.ncbar.gov/ethics/propeth.asp> (allowing use of cloud computing resources provided reasonable care is taken to minimize risks). On Jan. 20, 2011, the Ethics Committee withdrew Proposed Opinion 7, *Subscribing to Software as a Service While Fulfilling the Duties of Confidentiality and Preservation of Client Property*, for further study. *Id.*

put in place by the attorney.⁵⁹ Several opinions contemplate detailed communication, if not outright negotiation, with the service provider.⁶⁰ Others indicate that more than a working knowledge of and ongoing, informed review of the service provider's practices and policies is necessary.⁶¹

Examples of reasonable efforts to safeguard client confidential data include common measures such as the use of password-protection schemes and standard in-house firewall protection.⁶² Uncommon measures include: inspection of the vendor's privacy and confidentiality practices; notification to the vendor of the nature of the data stored on its servers; negotiation of a specialized agreement for sensitive data; and written assurances from the vendor that the client data is secure and only accessed on an as-needed basis.⁶³ Some state bars have suggested that the lawyer "actively manage" and ensure that the third-party "embraces" the lawyer's obligation to preserve client confidentiality.⁶⁴ However, none offer specific guidance on how to ensure the third-party fully embraces the lawyer's obligation or how to best actively manage the third-party relationship.

In 2006, the New Jersey Supreme Court Advisory Committee on Professional Ethics drew an analogy between client data that is physically located in a law firm and is potentially seen by outside support personnel, such as delivery or copy services, and client confidential data stored electronically on an off-site server.⁶⁵ The Advisory Committee recognized the same level of responsibility for each: the provider must: (1) know of the lawyer's duty of confidentiality; and (2) be enforceably contractually obligated, professionally or otherwise, to assist in preserving the confidentiality and security of client data.⁶⁶ The lawyer's "prudent professional judgment" that he has satisfied these criteria constitutes the exercise of reasonable care, according to the Committee.⁶⁷

In September 2010, the New York Committee on Professional Ethics, while approving use of cloud computing resources, cautioned lawyers to

59. See *supra* note 58 and accompanying text.

60. See Mass. Bar Ass'n Comm. on Prof'l Ethics, Formal Op. 05-04, *supra* note 58 (stating reasonable efforts could include receiving written assurances from the vendor regarding confidentiality of data obligations and drafting and agreeing on additional security measures as indicated by the nature of the data); Vt. Bar Ass'n Comm. on Prof'l Responsibility, Advisory Ethics Op. 03-03 on Client Confidences, *supra* note 58 (stating the lawyer must clearly communicate confidentiality rules to the vendor, explaining the rules so that the vendor understands and "embraces" the lawyer's obligation; the lawyer must determine if the vendor has "adequate safeguards" to protect client information).

61. See *Confidentiality; Maintaining Client Files; Electronic Storage; Internet*, Ariz. Comm. on the Rules of Prof'l Conduct, Op. 09-04, *supra* note 58 (stating that in conducting periodic review of the third-party service provider's reasonableness regarding online security precautions, the lawyer should exhibit "competence in the field of online computer security" or consult with an expert in the field); N.Y. Comm. on Prof'l Ethics, Op. 842, *supra* note 58 ("[T]he lawyer should stay abreast of technological advances to ensure that the storage system remains sufficiently advanced to protect the client's information . . .").

62. *E.g.*, Mass. Bar Ass'n Comm. on Prof'l Ethics, Formal Op. 05-04, *supra* note 58.

63. *Id.*

64. Vt. Bar Ass'n Comm. on Prof'l Responsibility, Advisory Ethics Op. 03-03 on Client Confidences, *supra* note 58.

65. N.J. Advisory Comm. on Prof'l Ethics, Op. 701, *supra* note 58.

66. *Id.*

67. *Id.*

actively monitor changing privilege laws concerning online storage so as to prevent jeopardizing or waiving any privilege protecting the data.⁶⁸ The Committee stated that the lawyer has a duty to keep current with technological advances so as to assess any risks or potential harm.⁶⁹ The variance between the existing opinions and the range of prescribed steps is too disparate to provide a sure foundation for the typical non-technologically savvy lawyer needing certainty about cloud computing use today.

C. Comments From the Bar, Judiciary, and Public

In response to the Commission's request for comment on its Technology Working Group Issues Papers, three hundred and thirty-three pages were received.⁷⁰ Among the notable submissions were those from prominent online legal blogger and creator of MyShingle.com, Carolyn Elefant,⁷¹ LexisNexis,⁷² the legal ethics counsel for the Advisory Committee of the Supreme Court of Missouri⁷³ and the ABA Standing Committee on Client Protection.⁷⁴ The commentators overwhelmingly agreed that rule-specific amendments would not be flexible enough to keep pace with rapid changes in technology and were therefore undesirable.⁷⁵ Commentators preferred development of an ABA online guide which would educate practitioners, identify best practices, and create baseline technology standards and model terms of service for cloud computing providers.⁷⁶ Ideally, the terms of service would include language regarding data ownership, accessibility of data, security, confidentiality, and privacy.⁷⁷ The ABA's considerable bargaining power was recommended as a way to secure prospective service provider compliance with specific terms of service. Development of an optional directory of ABA certified compliant vendors was also suggested.⁷⁸

68. N.Y. Comm. on Prof'l Ethics, Op. 842, *supra* note 58.

69. *Id.*

70. Technology Working Group Issues Papers, *supra* note 7.

71. Letter from Carolyn Elefant to ABA Comm'n on Ethics 20/20 (Dec. 15, 2010), Technology Working Group Issues Papers, *supra* note 7, at 13–44.

72. Letter from Jonah M. Paransky, VP Law Firm Practice Mgmt., LexisNexis, to ABA Comm'n on Ethics 20/20 (Dec. 16, 2010), Technology Working Group Issues Papers, *supra* note 7, at 179–85.

73. Letter from Sara Rittman, Legal Ethics Counsel, Advisory Comm. of the Supreme Court of Mo., to ABA Comm'n on Ethics 20/20 (Dec. 6, 2010), Technology Working Group Issues Papers, *supra* note 7, at 186–87.

74. Letter from ABA Standing Comm. on Client Protection to ABA Comm'n on Ethics 20/20 (Dec. 13, 2010), Technology Working Group Issues Papers, *supra* note 7, at 4–6.

75. *E.g.*, Letter from Legal Cloud Computing Ass'n to ABA Comm'n on Ethics 20/20 (Dec. 15, 2010), Technology Working Group Issues Papers, *supra* note 7, at 131–38.

76. *E.g.*, Letter from ABA Standing Comm. on Client Protection to ABA Comm'n on Ethics 20/20 (Dec. 13, 2010), Technology Working Group Issues Papers, *supra* note 7, at 4–6.

77. *Id.* The Legal Cloud Computing Association (LCCA) included suggestions for model terms of service in its comments. Letter from Legal Cloud Computing Ass'n to ABA Comm'n on Ethics 20/20 (Dec. 15, 2010), Technology Working Group Issues Papers, *supra* note 7, at 136–37.

78. Letter from Sara Rittman, Legal Ethics Counsel, Advisory Comm. of the Supreme Court of Mo., to ABA Comm'n on Ethics 20/20 (Dec. 6, 2010), Technology Working Group Issues Papers, *supra* note 7, at 186–87.

IV. RECOMMENDATION AND CONCLUSION

The creation of the ABA Commission on Ethics 20/20 and the degree of variance among state ethics committees' opinions recognize a degree of uncertainty in the implementation and usage of technology by lawyers. This is particularly true in view of the Model Rules' requirement to take reasonable efforts to safeguard client confidential data. Rapid changes in technology and improvement in data management render rules referencing specific technologies inadvisable. Any contemplated revisions⁷⁹ and modifications of the Model Rules should remove any reference to a "reasonable expectation of privacy"⁸⁰ with regard to modes of data transmission. The phrase is unhelpful and unnecessarily burdensome, especially absent binding precedent and in view of the lack of uniformity of interpretation as to when a reasonable expectation of privacy exists in electronic forms of communication and transmission of data. Additionally, the phrase potentially creates needless worry among members of the bar that they must either forego utilization of cloud computing resources or operate as early adopters of, and experts in, technology and security measures. Neither should be necessary or desirable.

Mirroring the New Jersey bar, the ABA should rather specify that prudent professional judgment with regard to storage of client confidential data in the cloud constitutes the exercise of reasonable care. In order to provide guidance for future legal rulings, the revised comment should note that typical use of cloud computing resources does not constitute either "sharing" or "disclosure" of client confidential data.

Cloud computing is already the standard model for consumer-oriented social sites; it is now gaining traction among businesses and governments seeking to leverage the flexibility, efficiency, and cost-effectiveness that large-scale pooling of data processing resources provides. Members of the bar are similarly situated to the public—the benefits of online data storage and access are apparent but the risks are not completely understood. The current state of interpretation suggests that lawyers must seemingly concern themselves with the underlying technology and policies of online server providers. Even given immediate and effective lawyer-consumer education, it is unlikely in the extreme that third-party service providers will consider tailoring their policies and practices in response to myriad understandings of a lawyer's professional obligation. Therefore, rather than imposing a requirement on members of the bar to be both technologically proficient and in constant communication and negotiation with service providers, the ABA is the logical choice to initiate discussion with third-party service providers and negotiate model terms of service, policies, and practices which will comport with developing ethical guidelines. In the meantime, while the Commission and the bar shape guiding principles over the next three years,⁸¹ the ABA should provide online

79. The Rules have not been significantly updated since 2002. MODEL RULES OF PROF'L CONDUCT Preface (2002).

80. MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. 17 (2002).

81. *Message from Commission on Ethics 20/20 Co-Chairs Jamie S. Gorelick and Michael Traynor*, *supra* note 3.

resources⁸² to enable lawyers to make informed decisions regarding the technology that is most safe, cost-effective, and beneficial for their unique practice situation.

82. The ABA currently provides a free guide to cloud computing for attorneys and suggested vendor questions which can serve as the foundation for the portal. *FYI: Software as a Service (SaaS) for Lawyers*, ABA, <http://www.abanet.org/tech/ltrc/fyidocs/saas.html> (last visited Mar. 8, 2011). In March, 2011, the ABA Center for Continuing Education sponsored a session on cloud computing eligible for 1.5 credits of CLE; registration costs for the ninety minute live webinar and teleconference ranged from \$90 for small businesses and solo practitioners to \$185 for the general public. *Security and Ethics of Cloud Computing*, ABA, <http://apps.americanbar.org/cle/programs/t11scc1.html> (last visited Mar. 8, 2011).