Western New England Law Review

Volume 37 *37 (2014-2015)*
Issue 2 *SYMPOSIUM—FIRM FOUNDATIONS: MANAGING THE SMALL FIRM AND INDIVIDUAL PRACTITIONER*

Article 5

2015

MASSACHUSETTS ATTORNEYS IN THE CLOUD— HOW MASSACHUSETTS REGULATIONS AND A CLASSIFICATION SYSTEM CAN PROVIDE MORE THAN A WISP OF GUIDANCE THROUGH THE FOG OF ETHICAL CLOUD COMPUTING

Daniel McKellick

MASSACHUSETTS ATTORNEYS IN THE CLOUD—HOW MASSACHUSETTS REGULATIONS AND A CLASSIFICATION SYSTEM CAN PROVIDE MORE THAN A WISP OF GUIDANCE THROUGH THE FOG OF ETHICAL CLOUD COMPUTING

DANIEL MCKELLICK, ESQ.*

INTRODUCTION

One hour—that is all it took to wipe away my digital storage in its entirety.[1] First, the hacker compromised and deleted my Google account.[2] Then, he broke into my Twitter account and posted hateful messages under my name. Finally, the hacker conducted the worst breach of all—my Apple ID account. Once my Apple ID was compromised, the hacker remotely erased all the data on my MacBook, iPad, and iPhone. Everything was gone. How could this happen to me? I write for a technology periodical. I attend tradeshows and look for new developments in technology. My job is to know technology, the gadgets, and the proper use of these products.

How was this done? Through the cloud, where one's data is stored on a cloud vendor's server and can be accessed with an Internet

* Attorney at Bacon Wilson, P.C., Springfield, Massachusetts. I would like to thank the organizers of the solo and small firm symposium. In my early career, I was involved in small business management and received a degree in Business Management from the UMass Isenberg School of Business and, as such, the topic of the symposium has a special place in my heart. I would also like to thank the staff of the Western New England Law Review. As a previous member, I remember all of hard work required to meet deadlines. Additionally, many thanks go to the staff of the Law Library at Western New England for their continuing support and assistance. Finally, I dedicate this piece to my wife, Melissa, and our children, Daniel, Liam, and Cailin, for without their support and understanding my journey into the legal profession would have never commenced.

1. This is not a hypothetical, but a true story of how cloud hacking can affect an individual. The story, as laid out here, is a summary of an extensive story on how the hackers accessed the victim's accounts and how the victim discovered how the hacker did it. Mat Honan, *How Apple and Amazon Security Flaws led to My Epic Hacking*, WIRED (Aug. 6, 2012, 8:01 PM), http://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/ (describing how the cloud based accounts of a senior writer for multiple technology based media sources accounts were hacked and all of the information deleted).

2. *Id.*

connection and the appropriate user credentials.[3] Once accessed, all of the data that is stored within that account is not only accessible but also erasable.

Despite the potential for catastrophic repercussions, the use of cloud computing in the legal profession is rising and more attorneys are using this technology every day.[4] Law firms use the cloud for practice management, e-discovery, and document management.[5] The traditional system of servers and support[6] are "wasteful, inefficient, and expensive."[7] The economics of computing creates a natural progression to transition into the cloud,[8] and, in business, cloud computing is the wave of the future.[9]

Despite an increasing reliance on cloud computing, there remains a prevailing uncertainty among lawyers behind the technology of the cloud.[10] Rules governing the technology, and how the technology applies to an attorney's professional obligations, are in their infancy.[11] As a result, "the overall lack of guidance" regarding the cloud has caused many attorneys to fear the "potential ramifications of storing confidential client files" in the cloud.[12]

Naturally, attorneys have turned to their state bar associations for guidance on how to capitalize on the benefits of the cloud while maintaining their professional obligations. In response, ethics committees have permitted the use of the cloud and issued a reasonableness standard to govern the attorneys' conduct.[13] In general, this standard permits the storage of confidential client information so

3. *Id.*

4. *See* NICOLE BLACK, CLOUD COMPUTING FOR LAWYERS 13 (ABA 2012).

5. Catherine Sanders Reach, *Reach for the Cloud*, TRIAL, Jan. 2012, at 38-9.

6. *Id.* at 39-40.

7. BLACK, *supra* note 4, at 6.

8. *Id.*

9. *Id.* at 6-7.

10. *See id.* at 27-28.

11. *Id.* at 27.

12. *Id.*

13. *See* N.C. State Bar, 2011 Formal Op. 6, ¶ 12 (2012) (reasonable care); Iowa State Bar Ass'n Committee on Ethics & Pract. Guidelines, Formal Op. 11-01, at 2 (2011) (due diligence); Vt. Bar Ass'n Prof'l Responsibility Section, Formal Op. 2010-6, at 6 (2011), *available at* https://www.vtbar.org/FOR%20ATTORNEYS/Advisory%20Ethics%20Opinion.aspx (due diligence); N.Y. State Bar Ass'n Committee on Prof. Ethics, Formal Op. 842, ¶ 13 (2010), *available at* https://www.nysba.org/CustomTemplates/Content.aspx?id=1499 (reasonableness standard); State Bar of Ariz., Formal Op. 09-04, ¶ 13-14 (2009), *available at* http://www.azbar.org/Ethics/EthicsOpinions/ViewEthicsOpinions?id=704 (reasonable precautions).

long as attorneys perform reasonable steps to protect against property loss and inadvertent or unauthorized disclosure of confidential information.[14] Reasonableness also requires attorneys to act with due diligence to protect the information from threats.[15]

Beyond reasonableness, ethics committees provide varying levels of guidance on how attorneys can meet their professional obligations. Some ethics opinions offer suggestions of what reasonableness may require.[16] These mandatory requirements have been subject to criticism because of the belief that their rigidity makes them unworkable with ever-changing technologies.[17] Instead, those critics prefer that ethics committees apply a blanket "reasonableness" standard to all cloud storage because it allows attorneys to be more adaptable to the fast-paced changes in technology.[18]

The guidance on how attorneys can meet their professional obligations while using the cloud has been limited by the use of the reasonableness standard. The purpose of this piece is threefold: to provide a general background on the cloud and its application in the practice of law; to identify issues that Massachusetts attorneys should be aware of before introducing the use of cloud computing into their business model; and to provide other possible sources, beyond the ethics committees opinions, where attorneys who wish to meet their professional obligations while storing their clients' information in the cloud can turn.

Part I of this piece provides a broad overview of cloud computing, the rules of professional responsibility primarily implicated, the benefits of the cloud, and the risks attorneys face. Part II lays out how several ethics committees responded to the concerns raised by attorneys. In Part III, this piece analyzes the Massachusetts opinion,[19] showing how the reasonableness standard alone can be misleading and how

14. *See* N.C. State Bar, 2011 Formal Op. 6, ¶ 124 (2012); Pa. Bar Ass'n Committee. on Legal Ethics & Prof. Resp., Formal Op. 2011-200, at 6-7 (2010).

15. *See* State Bar of Ariz. Formal Op. 09-04, ¶ 1,14 (2009), *available at* http://www.azbar.org/Ethics/EthicsOpinions/ViewEthicsOpinions?id=704; N.J. State Bar Ass'n Advisory Committee on Prof. Ethics, Formal Op. 701, ¶ 15 (2006).

16. *See* N.Y. State Bar Ass'n Committee on Prof. Ethics, Formal Op. 842, ¶ 13 (2010) *available at* http://www.nysba.org/CustomTemplates/Content.aspx?id=1499 (requiring that the attorney must monitor any change in law as it pertains to cloud computing and privilege of protecting the information); *see also* N.C. State Bar, 2011 Formal Ethics Op. 6, ¶ 15-21 (2012).

17. *See* BLACK, *supra* note 4, at 6.

18. Letter from Nicole Black, Attorney, to Alice Neece Mine, N.C. State Bar (Apr. 9, 2010) (on file with author).

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

reasonableness alone falls short of providing sufficient guidance to Massachusetts attorneys who seek to satisfy their professional responsibilities while using the cloud. In Part IV, this piece directs Massachusetts's attorneys to consumer protection regulations that actually provide a better framework for the attorney that wishes to investigate cloud use and use the cloud in a manner that is compliant with the rules of professional responsibility. Furthermore, this section establishes a classification system that will allow practitioners to tailor their due diligence inquiry based on how they use the cloud in their practice.

I. TRENDING NOW: ATTORNEYS EXPLORE CLOUD COMPUTING OPTIONS FOR THEIR PRACTICE

Cloud computing is a way of accessing data that is stored at a remote location.[20] As attorneys explore cloud storage solutions for their client files, questions arise as to how this remote storage option relates to their professional obligations.[21] Although there are many benefits to using the cloud, this technology also carries inherent risks.[22]

A. *What is Cloud Computing?*

Cloud computing is "a sophisticated form of remote electronic data storage on the Internet."[23] Traditionally, data is stored locally or on a server located within the business.[24] In contrast, the cloud stores data on large remote servers maintained by an outside vendor.[25] The vendor is responsible for the information technology (IT) infrastructure, the storage, and the maintenance of the servers.[26] Users of the cloud can remotely access the data stored on the vendor's server from anywhere

20. *See* Reach, *supra* note 5, at 38.

21. BLACK, *supra* note 4, at 35-6.

22. *See* SHARON D. NELSON ET AL., LOCKED DOWN 119 (ABA 2012); *see also infra* Part I.D. Some risks of cloud computing include privacy, loss of data and security. *See generally* BLACK, *supra* note 4, at 26-31; Pa. State Bar Ass'n Committee on Legal Ethics & Prof. Resp., Formal Op. 2011-200 (2010).

23. Richard Acello, *Get Your Head in the Cloud*, 96 A.B.A. J., Apr. 2010, at 28, 28. It is challenging to find a universal definition of cloud computing. NELSON ET AL., *supra* note 22, at 121. *See generally Cloud Computing for Lawyers*, A.B.A., http://www.abanet.org/tech/ltrc/fyidocs/saas.html (last visited Apr. 14, 2015) (providing some background information on cloud computing with software as a service (SaaS)).

24. *See* Acello, *supra* note 23, at 29. Local storage is data that is stored on the hard drive of the computer.

25. *Id.* at 28.

26. *See* Reach, *supra* note 5, at 40 (saving a law firm the cost of providing their own servers, storage, maintenance, support, and security).

there is an Internet connection.[27] Additionally, cloud storage allows access to stored data from multiple devices such as laptops and cell phones.[28]

In 2007, the legal profession's use of cloud computing increased because a few cloud vendors entered the marketplace with software tailored for the practice of law.[29] Although the legal profession is traditionally slow in embracing new technologies, there is evidence showing that a growing number of attorneys are using, or inquiring into, cloud computing options.[30] Attorneys are attracted to the low cost of the service; in fact, some cloud vendors provide free data storage.[31] Despite the increase in use, many attorneys remain uncertain on how cloud use affects their professional responsibilities.[32]

B. *How Cloud Computing Relates to an Attorney's Ethical Responsibilities*

Cloud computing implicates multiple rules of the Model Rules of Professional Conduct (MRPC).[33] There are, however, three primary rules that relate to an attorney's use of cloud storage.

First, Rule 1.1 obligates the attorney to "provide competent representation."[34] Part of this obligation requires the attorney to have the requisite "legal knowledge [and] skill" that is reasonably necessary to

27. Acello, *supra* note 23, at 28. Individuals who have accounts with Google, Yahoo, Facebook, LinkedIn, or Netflix are aware of how flexible account access is. These programs are all cloud based. *See* BLACK, *supra* note 4, at 1.

28. Brian Chase, *Law Office Technology: Are We Safe in the Cloud?*, 49 AZ ATTORNEY, Oct. 2012, at 38, 38. In fact, while the cloud has been around for many years, the rise in its popularity is attributed, in part, to the increase in the use of mobile devices because the mobile workforce requires instant access to data. Reach, *supra* note 5, at 39.

29. *See* BLACK, *supra* note 4, at 13. *See also* LEGAL CLOUD COMPUTING ASSOCIATION, http://www.legalcloudcomputingassociation.org/Home/netdocuments-nextpoint-and-dialawg-join-legal-cloud-computing-association (last visited Apr. 14, 2015) [hereinafter *LCCA*] (announcing the increase in size to seven cloud vendor members).

30. BLACK, *supra* note 4, at 12-13.

31. *Compare* CLIO, http://www.goclio.com/signup/ (last visited Apr. 14, 2015) (stating that the monthly fee for an attorney is forty-nine dollars and support staff is twenty-five dollars per month), *with* Chase, *supra* note 28, at 38 (describing programs such as Dropbox and Google Docs as cloud based storage systems that allow users to store data at no charge).

32. BLACK, *supra* note 4, at 27-8.

33. For purposes of this piece, the author uses the ABA Model Rules of Professional Conduct. Although the Massachusetts rules are a modified version of an earlier MRPC, it is reasonable to assume that when evaluating cloud computing standards, committees will need to look to the newer versions of the MRPC because they address the use of such technologies. That said, attorneys should consider all previous rule-specific opinions issued by their respective ethics committees to be sure their technology use complies with those opinions.

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

provide representation.[35] A recent update to this Rule[36] requires the attorney to stay abreast of "the benefits and risks" of technology, like cloud computing, in order to maintain the requisite knowledge and skill.[37]

Next, Rule 1.6 deals with confidentiality, and is at the center of all of the ethics opinions on cloud computing. In part, Rule 1.6 requires the attorney to obtain informed consent before "reveal[ing] information relating to the representation of a client . . . . "[38] This is a key provision because cloud-computing attorneys store their data on remote servers, to which the employees of the cloud vendor may have access.[39] The ABA recently revised this Rule also,[40] and comment eighteen requires attorneys to make reasonable efforts to prevent unauthorized access to, or inadvertent disclosure of, a client's information.[41] In order to determine what is reasonable, some factors that the attorney needs to consider are "the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, and the difficulty of implement[ation]."[42] Confidentiality is a key concern because cloud computing inherently brings with it the risk of unauthorized access and inadvertent disclosure.[43]

Finally, Rule 1.15 governs the safekeeping of a client's property.[44] Property includes the client's records and documents that are stored within the attorney's file.[45] The obligation to safeguard property requires the attorney to preserve the client's property for a period of

35. *Id.*

36. ABA Comm. on Ethics 20/20, Resolution-105A Revised (2012), *available at* www.americanbar.org/content/dam/aba/administrative/ethics_2020/20120808_revised_resolution_105a_as_amended.authcheckdam.pdf [hereinafter *ABA Resolution*].

37. MODEL RULES OF PROF'L CONDUCT R. 1.1 cmt. 8 (2013), *available at* www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_1_competence/comment_on_rule_1_1.html.

38. MODEL RULES OF PROF'L CONDUCT R. 1.6(a) (2012). The rule provides a specific list of exceptions to the consent requirement and states "disclosure is impliedly authorized in order to carry out the representation." *Id.*

39. *See* Pa. State Bar Comm. on Legal Ethics & Prof. Resp., Formal Op. 2011-200, at 1 (2010) (discussing how employees that work for the cloud vendor may have access to the material and how that access can adversely impact both competency and confidentiality).

40. ABA Resolution, *supra* note 36.

41. MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. 18 (2013), *available at* www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_6_confidentiality_of_information/comment_on_rule_1_6.html.

42. *Id.*

43. *See infra* Part I.D.

44. MODEL RULES OF PROF'L CONDUCT R. 1.15 (2012).

45. Ala. State Bar Ethics Op. 2010-02, at 4 (2010).

"five" years.[46] Cloud computing creates potential violations of Rule 1.15 because of the risk of data loss.[47] Accordingly, attorneys aim to uphold their ethical obligations while availing themselves of the various benefits of cloud usage.

C. *The Benefits of Cloud Computing*

The cloud model is not only convenient for attorneys, but it is also cost effective.[48] Law firms save money by not having to provide the hardware, software, and maintenance a traditional system requires because the cloud vendor provides the servers and updates the software.[49] In general, cloud vendors charge only a monthly fee, which allows most small firms to realize a low entry cost into high capacity data storage.[50]

Moreover, cloud computing provides flexibility for the attorney.[51] For example, some legal software programs are designed for Windows and are not compatible with Macintosh computers.[52] The cloud has no compatibility issues because cloud vendors deliver their service through the Internet. A startup firm can particularly benefit from this model so long as it has a computer with the appropriate operating system and an Internet connection.[53]

Additionally, a cloud vendor provides attorneys with exponentially more storage space than a local server.[54] The cloud vendor can also serve as an off-site data backup in the event that an attorney's local

46. MODEL RULES OF PROF'L CONDUCT R. 1.15(a) (2012). The length of time for preservation of the client's property varies; for example, Alabama requires six years because that is the statutory limit for the client to bring an action against the attorney. *See* Ala. State Bar Ethics Op. 2010-02, at 10 (2010).

47. *See infra* Part I.D. The risk of data loss is not limited to unauthorized intruders, but can also occur if the cloud vendor goes out of business.

48. *See* Reach, *supra* note 5, at 40.

49. *Id.*

50. *Id.* In general, vendors that charge for their service apply a monthly fee per user. *E.g.*, CLIO, *supra* note 31. The monthly costs continue for the duration of use. A traditional system generally will have a large upfront cost, but lower operating costs. Thus, depending on the cost of a traditional system and the number of users, the cloud cost can exceed that of traditional system over an extended time because the monthly costs continue until use is terminated.

51. BLACK, *supra* note 4, at 22.

52. *Id.* Locating practice management applications for a Macbook pro can be challenging. *See* E-mail from Timothy Evans, Attorney, to Alice Mine, N.C. State Bar (Apr. 7, 2010 12:08 EST) (on file with author) (sharing his difficulties finding practice management software and his decision to use a cloud vendor).

53. *See* BLACK, *supra* note 4, at 22; Evans, *supra* note 52 (stating one only needs to remember their username and password to access from any computer).

54. *See* BLACK, *supra* note 4, at 22.

storage crashes.[55] These are just some of the benefits an attorney can obtain from using the cloud. Of course though, with the benefits also come risks.

D. *The Risks the Cloud Presents to Attorneys and Clients*

Irresponsible cloud use can lead to a security breach and temporary or permanent loss of data.[56] Some cloud storage security breaches have a *de minimis* impact, while others come with larger repercussions.[57] Nevertheless, either degree of loss leads to compromised data.[58] Accordingly, attorneys should carefully consider the risks of cloud computing before using it for data storage.[59]

Cloud storage carries a genuine risk of unauthorized access.[60] As noted throughout this section, high profile security breaches suggest that the risks "are not speculative, trivial, or financially insignificant."[61] A security breach into a firm's cloud storage can provide the intruder with access to all the files stored with the cloud vendor.

Breach of a cloud computing system is not limited to random attacks. In 2009, the FBI issued an advisory stating that hackers are targeting law firms for both identity theft and espionage purposes.[62] In fact, a firm that was involved in litigation against a foreign nation was the victim of a major breach.[63] The thieves managed to obtain the credentials of over thirty users and accessed thousands of emails that

55. *Id.* at 25.

56. *See id.* at 26-32. Some businesses prefer to stay away from the cloud storage because of questions of accountability for safeguarding information. *See* Meridith Levinson, *Software as a Service (SaaS) Definition and Solutions*, CIO.COM (May 15, 2007, 8:00 AM), http://www.cio.com/article/2439006/web-services/software-as-a-service—saas—definition-and-solutions.html.

57. *Compare* Heather Kelly, *Apple Account Hack Raises Concern about Cloud Storage*, CNN, (Aug. 7, 2012, 5:29 AM), http://www.cnn.com/2012/08/06/tech/mobile/icloud-security-hack/ (hacked cloud account provided the intruder with the account holders personal information), *with* Roland L. Trope & Sarah Jane Hughes, *Red Skies in the Morning-Professional Ethics at the Dawn of Cloud Computing*, 38 WM. MITCHELL L. REV. 111, 181-82 (2011) (hacked Sony online gaming system delivered through the cloud where user information for seventy-seven million customers was obtained, costing the company billions of dollars).

58. *See supra* text accompanying note 56.

59. *See also* Penn. State Bar Comm. on Legal Ethics and Prof'l Responsibility, Formal Op. 2011-200 (2010); BLACK, *supra* note 4; NELSON ET AL., *supra* note 22 (providing more background on the risks of cloud computing in legal practice see).

60. Mass. State Bar Comm. on Prof'l Responsibility, Formal Op. 2012-0003, ¶ 9 (2012).

61. Trope & Hughes, *supra* note 57, at 123-24.

62. NELSON ET AL., *supra* note 22, at xviii.

63. *Id.* at 10. Only limited information is available on this breach because the security company had a confidentiality agreement with the law firm.

were stored on the servers.[64] This was only the start because the intruders had access to all of the servers and computers on the network.[65]

Proper training on security risks can aid firms in defending against security breaches. For example, a firm in Los Angeles survived a targeted phishing scheme because of its security awareness.[66] The firm had filed a large copyright infringement suit and, immediately after filing, started to receive suspicious emails.[67] The firm conducted an investigation and found that the emails, which appeared to be sent from within the firm, contained malware that seemed to originate in China.[68] Training played a key role in thwarting the intruder because the organization was able to identify the threat, communicate it effectively throughout the firm, and, as a result, the malware bomb did not impact the system because no one opened the email.[69]

Recent cloud data breaches across multiple industries have cost companies millions of dollars and "have increased concerns about data security for cloud services."[70] Cloud users' security concerns focus on "the lack of security controls in place to protect customer data."[71] To complicate matters more, a recent report determined that a majority of "cloud providers don't think [security controls are] their job."[72]

A security breach could result in a client's file being compromised or deleted. This can harm the firm's reputation and disclose confidential client information, which may result in a legal action against the firm. Because of these security risks, attorneys have sought guidance from their state bar associations on how cloud computing and attorneys' professional obligations can work simultaneously.

II. STARTING UP: ETHICS COMMITTEES ATTEMPT TO CONNECT PROFESSIONAL RESPONSIBILITY TO THE CLOUD

To date, a handful of ethics opinions have addressed how attorneys can meet their ethical obligations while using the cloud.[73] All of the

64. *Id.*
65. *Id.*
66. *Id.* at 9.
67. NELSON ET AL., *supra* note 22, at xviii.
68. *Id.*
69. *Id.* at 9-10.
70. Pa. State Bar Comm. on Legal Ethics and Prof'l Responsibility, Formal Op. 2011-200, at 3 (2011).
71. Trope & Hughes, *supra* note 57, at 195.
72. *Id.*
73. Travis Pickens, *Ethics up in the Clouds*, 81 OKLA. B. J., Nov. 2010, at 2407; *see* AMERICAN BAR ASSOCIATION, *Cloud Ethics Opinions Around the U.S.*, http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resource

ethics committees concluded that attorneys may use cloud storage for confidential client information and issued a "reasonableness" standard to aid attorneys in fulfilling their professional obligations.[74] In addition to "reasonableness," the opinions offer various levels of guidance to attorneys.

A. *The Reasonableness Standard as Applied to the Cloud*

The MRPC define "reasonableness" as the "conduct of a reasonably prudent and competent lawyer."[75] In general, the ethics committees have determined that attorneys can store confidential information in the cloud so long as they exercise reasonable steps to protect against inadvertent or unauthorized disclosure of a client's confidential information and property loss.[76] This standard does not create an obligation to establish an impenetrable storage system, but it does require the attorney to act with due diligence to secure the client's information against foreseeable data breaches.[77] Thus, the reasonableness standard applies to the selection of a cloud vendor and to ongoing security practices of vendors and attorneys.[78]

B. *Guidance Beyond Reasonable Care*

Beyond reasonableness, the amount of guidance provided by ethics committees has varied. An early opinion on remote data storage offered limited guidance on how attorneys can meet their ethical obligations under the reasonableness standard.[79] Beyond the reasonable precautions to protect the security and confidentiality of the client's information, the committee only stated that attorneys "should" be aware of their "competence regarding online security" and "may" need to review their security measures periodically.[80] The guidance offered is limited because the opinion fails to specify any potential security threats that require "awareness" or what types of security measures attorneys should

s/charts_fyis/cloud-ethics-chart.html (last visited Apr. 14, 2015) (listing the states that have an ethics opinion related to cloud computing).

74. *See* Bob Ambrogi, *Mass. Joins Other States in Ruling that Cloud Computing is Ethical for Lawyers*, CATALYSTSECURE.COM, (July 5, 2012), http://www.catalystsecure.com/blog/2012/07/mass-joins-other-states-in-ruling-that-cloud-computing-is-ethical-for-lawyers/.

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

76. *See* State Bar N.C., 2011 Formal Ethics Op. 6, ¶ 4 (2012); Pa. State Bar Comm. on Legal Ethics and Prof'l Responsibility, Formal Op. 2011-200, at 1 (2010).

77. *See* State Bar of Ariz. Formal Ethics Op. 09-04, ¶ 1 (2009); N.J. State Bar Ass'n Advisory Comm. of Prof'l Ethics, Op. 701, ¶ 13 (2006).

78. N.J. State Bar Ass'n Advisory. Comm. of Prof'l Ethics, Op. 701, ¶ 13 (2006).

79. State Bar of Ariz. Formal Ethics Op. 09-04, ¶ 1 (2009).

80. *Id.*

consider.

More recently, ethics opinions have provided "basic" guidance by identifying potential areas of ethical concern within the cloud.[81] The Iowa opinion laid out six sets of questions illustrating concerns that attorneys should have when selecting a cloud vendor.[82] The areas addressed are access to data, legal issues with data storage, financial obligations, termination of relationship, password protection and access, and data encryption.[83] The questions help to provide some guidance to attorneys in the vendor selection process.

Similarly, the Massachusetts opinion provides a five-item list that identifies some areas of concern when selecting a vendor; however, the opinion does not set forth specific questions.[84] The Massachusetts Committee designed this list in order to determine if the cloud provider's terms of use, policies, and procedures are compatible with the attorney's professional obligations.[85]

Likewise, the Vermont opinion sets forth a list of broad vendor-specific concerns which the attorney should have a "reasonable understanding of" in order to perform due diligence.[86] The Vermont Committee, however, expressed that it is "not appropriate to establish a checklist of factors a lawyer must examine."[87]

Attempting to alert attorneys to the breadth of cloud issues, the Pennsylvania Ethics Committee provided a detailed list of what the "reasonable care" standard "may" include.[88] All told, there are thirty-one bullet points that address issues related to attorneys using cloud storage.[89] The list contains items that address vendor selection, vendor security, and attorney security.[90] As a result, the list provides attorneys with a solid framework as to how they should investigate cloud-

81. *See* Iowa State Bar Ass'n Ethics & Practice Comm., Formal Op. 11-01, 2 (2011) (describing the level of guidance as "basic ").

82. *Id.* For example, "[W]ill I have unrestricted access to stored data?" In addition, if the relationship terminates, "[H]ow do I retrieve my data and does the SaaS company retain copies?" *Id.* at 2-3.

83. *Id.*

84. Mass. State Bar Comm. on Prof'l Responsibility, Formal Op. 2012-0003, ¶ 7 (2012).

85. *Id.* at ¶ 1; *see also infra* Part III.

86. Vt. Bar Ass'n Prof'l Responsibility Section, Formal Op. 2010-6, ¶ 19 (2011).

87. *Id.*

88. Pa. State Bar Comm. on Legal Ethics and Prof'l Responsibility, Formal Op. 2011-200, 8-10 (2010).

89. *Id.*

90. *Id.*

computing options in order to meet their ethical obligations.[91]

Opinions that identify issues by recommending questions that attorneys should ask provide some guidance.[92] However, the guidance can be inconsistent based upon how attorneys perceive the questions, since recommendations can be interpreted as mandatory requirements, mere suggestions, or something that can be disregarded because it is not required.[93]

In order to provide direct guidance, several opinions use mandatory requirements to guide attorneys in meeting their ethical obligations. For example, to meet the competence obligation some opinions require "regular education" in cloud computing[94] or "stay[ing] abreast of technological advances."[95] Security takes center stage in Alabama where attorneys "must" stay abreast of "appropriate security safeguards" employed by both the attorney and the provider.[96] Moreover, the Alabama opinion requires attorneys "to become knowledgeable about how the provider will handle the storage and security of the data being stored."[97] In New Jersey, the "touchstone in using 'reasonable care'" requires, in part, that the provider have an "enforceable obligation" to preserve confidentiality and security.[98] Mandatory requirements such as these set forth clear benchmarks that allow attorneys to understand what they must do in order to fulfill their ethical obligations.

Despite their clarity, mandatory requirements have met stiff resistance. For example, in North Carolina the reasonableness standard

91. *Id.* at 11-19. This opinion includes a section on cloud-based email, and provides summaries of other states' opinions on issues of remote data storage. *Id.*

92. The opinions vary in that some merely direct attorneys to ask questions while others clearly articulate that attorneys should have an understanding of the items set forth. *Compare* Iowa State Bar Ass'n Ethics & Practice Comm., Formal Op. 11-01, at 2 (2011) (providing a list of questions), *with* Vt. Bar Ass'n Prof'l Responsibility Section, Formal Op. 2010-6, ¶ 19 (2011) (directing attorneys to have a reasonable understanding of the items set forth).

93. *See* BLACK, *supra* note 4, at 38. Furthermore, attorneys are not only seeking what questions to ask but also what answers they should be looking for. *See* Letter from Neil A. Riemann, Lawyer, to Alice Neece Mine, N.C. State Bar (Dec. 16, 2010) (on file with author) (looking for guidance and not a list of questions that attorneys will not know the answers to or understand the answers a vendor may give them).

94. State Bar N.C., 2011 Formal Ethics Op. 6, ¶ 13 (2012).

95. N.Y. State Bar Ass'n Comm. on Prof'l Ethics, Formal Op. 842, ¶ 10 (2010).

96. Ala. State Bar Ethics Op. 2010-02, 16 (2010).

97. *Id.*

98. N.J. State Bar Ass'n Advisory. Comm. of Prof'l Ethics, Op. 701, ¶ 13 (2006); *see also* N.Y. State Bar Ass'n Comm. on Prof'l Ethics, Formal Op. 842, ¶ 9 (2010) (listing an "enforceable obligation" with the cloud vendor as a suggestion to what reasonable care might include).

was established after a series of proposed opinions,[99] one of which contained an extensive list of proposed mandatory requirements.[100] The requirements included provisions to examine the vendor's financials, determine the location of the vendor's servers and the jurisdiction's seizure requirements, and to require the vendor to protect the data stored as a fiduciary.[101] The Committee sent the proposed opinion out for commentary and received feedback from proponents and opponents of the mandatory requirements.[102] In the end, the Committee dropped the proposed requirements and issued a "due diligence" standard for security measures, with a mandatory education provision.[103]

III. LIMITED CONNECTION: REASONABLENESS FAILS TO IDENTIFY THE ISSUES AND PROVIDE GUIDANCE

The cloud computing reasonableness standard and the application of proposed tests can mislead attorneys into a false sense of security. In a recent opinion on cloud computing, the Massachusetts Ethics Committee provided a list of factors that may be included in "reasonable efforts" to ensure that the vendor's practices are compatible with the attorney's professional obligations.[104] The Committee's conclusion and a full application of the Committee's test appear to be inconsistent with each other.[105] Additionally, the opinion is very narrow in scope because it only addresses the vendor selection process.[106] These two shortcomings in the opinion can mislead attorneys, and make them vulnerable to a security breach or a data loss.

The issue presented to the Committee was whether a lawyer violates his professional obligations when storing "confidential client information using Google [D]ocs or some other internet based storage solution . . . ."[107] The Committee concluded that the attorney could use

99. *See* State Bar N.C., 2011 Proposed Ethics Op. 6 (2011); State Bar N.C., 2011 Proposed Ethics Op. 7 (2011); State Bar N.C., 2010 Proposed Ethics Op. 7 (2010) (these three proposed opinions were merged into the final opinion).

100. State Bar N.C., 2010 Proposed Ethics Op. 7 (2010).

101. *Id.*

102. Timeline of 2011 FEO 6 and 2011 FEO 7, State Bar N.C. (2012) (on file with the State Bar N.C.).

103. *See* State Bar N.C., 2011 Formal Ethics Op. 6, ¶ 5 (2012).

104. Mass. Bar Comm. on Prof'l Responsibility, Formal Op. 2012-0003, ¶ 7 (2012), *available at* http://massbar.org/publications/ethics-opinions/2010-2019/2012/opinion-12-03.

105. *See id.*

106. *Id.*

107. *Id.* ¶ 2. The opinion lists separately Windows Azure, Apple iCloud, and Amazon S3 as other cloud base storage options. *Id.*

Google Docs to store confidential information,[108] so long as the attorney makes "reasonable efforts" to be sure that the vendor's terms of use, policies, and procedures (TUPP) are compatible with the attorney's professional obligations.[109] The Committee then set forth five items that "reasonable efforts" would include.[110]

The Committee's conclusion, allowing the use of Google Docs to store confidential information, however, is a mystery because when the five factors are applied to the TUPP, Google Docs fails to meet the criteria of "reasonable efforts."[111] For example, the second provision of the opinion states that the TUPP should ensure that the provider "prohibit[s] unauthorized access to data stored on the provider's system, including access by the provider itself for any purpose other than conveying or displaying the data to authorized users."[112] Accordingly, the attorney must make certain that the cloud vendor only accesses the stored data in order to display it to the attorney.[113]

The language of the Google TUPP, however, provides reason for concern because it allows room for unauthorized access to confidential information.[114] When an attorney uploads to Google, the attorney gives Google a license to host, store, reproduce, and communicate the information in order to operate, promote, and improve its services.[115]

108. "The Committee believes that the reasoning set forth . . . would allow Lawyer . . . to use Google docs . . . to store confidential client information . . . ." *Id.* ¶ 7.

109. *Id.* The Committee relied on opinions 00-01 (unencrypted email) and 05-04 (third-party software vendor) to support this conclusion. *Id.* ¶ 7.

110. *Id.* First, the attorney must examine the TUPP "with respect to data privacy and the handling of confidential information." Second, the attorney must "ensure" that the TUPP "prohibit[s] unauthorized access to data stored on the provider's system, including access by the provider itself for any purpose other than conveying or displaying the data to authorized users." Third, the TUPP should ensure that the lawyer has reasonable access, and control over the data stored, in the event that one party dissolves the relationship. Fourth, the attorney should examine the vendor's practices and history "to reasonably ensure that the data stored on the provider's system actually will remain confidential." Finally, the attorney should periodically reexamine the TUPP to ensure that the use remains "compatible with Lawyer's professional obligations to protect confidential client information reflected in Rule 1.6(a)." *Id.*

111. *Id.* The list suggests that all five steps must be taken because the multi-element construction uses "and" between the last two criterion; therefore the list should be read as a conjunctive list. ANTONIN SCALIA & BRYAN A. GARNER, READING LAW: THE INTERPRETATION OF LEGAL TEXTS, 116-18 (2012).

112. Mass. Bar Comm. on Prof'l Responsibility, Formal Op. 12-03, ¶ 7 (2012), *available at* http://massbar.org/publications/ethics-opinions/2010-2019/2012/opinion-12-03.

113. The attorney or another authorized user. *Id.*

114. MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. 18 (2013), *available at* www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_6_confidentiality_of_information/comment_on_rule_1_6.html.

115. *Google Terms of Service*, GOOGLE, http://www.google.com/intl/en/policies/terms/ (last modified Apr. 14, 2014).

The words "operate"[116] and "improve,"[117] suggest that the information will stay within the company, but the word "promote,"[118] allows the data stored to be used for marketing purposes. This risk of unauthorized access is magnified when one considers that Google provides its services free of charge and makes its money through advertising.[119] Google's reserved right to access information for reasons other than displaying it to the attorney creates a risk of violating the attorney's confidentiality obligation.[120]

Furthermore, the third "reasonable effort" criterion states that the TUPP should ensure that the lawyer has reasonable access to and control over the data stored.[121] Alarmingly, the language of the TUPP does not guarantee that the attorney will have access to the information stored if the relationship terminates. It reads that Google may suspend a user's access and create new limits on the service.[122] Additionally, Google Docs may suspend the service altogether, with or without notification.[123] These terms show that attorneys may be at risk of losing all of their data in the event of service termination.[124] Google Docs does not fulfill this requirement because attorneys cannot make certain that they have access to their stored data, and this can violate their obligation to safeguard client property.[125]

Despite the failure of Google Docs to meet the criteria established by the Massachusetts Ethics Committee, the Committee authorized the use of Google Docs to store confidential information.[126] This result is misleading and may cause confusion among attorneys that are reviewing a vendor's TUPP while exploring cloud-computing options. If attorneys rely on a TUPP that is similar to that of Google Docs, then the attorneys may be at risk of violating their professional responsibilities of

116. *Id.*
117. *Id.*
118. *Id.*
119. *Id.*
120. MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. 18 (2013), *available at* www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_6_confidentiality_of_information/comment_on_rule_1_6.html.
121. Mass. Bar Comm. on Prof'l Responsibility, Formal Op. 12-03, ¶ 7 (2012), *available at* http://massbar.org/publications/ethics-opinions/2010-2019/2012/opinion-12-03 (stating that data control is critical in the event that one party dissolves the relationship).
122. Google, *supra* note 115. Additionally, in the event of cancellation Google retains the right to access the data. *Id.*
123. *Id.*
124. Additionally, the terms do not specify any alternative method of backup retrieval. *Id.*
125. MODEL RULES OF PROF'L CONDUCT R. 1.15 (2012).
126. Mass. State Bar Comm. on Prof'l Responsibility, Formal Op. 2012-0003, ¶ 1 (2012).

confidentiality and the safeguarding of property.[127]

Another area of concern raised by the Massachusetts opinion is the Committee's limitation of the attorney's inquiry to the vendor and failure to provide guidance on how to protect confidential information on the user's side. For example, the Committee did not mention issues such as user access, data backup for confidential information, or any security measures. By limiting the "reasonable efforts" inquiry to the vendor,[128] the opinion could mislead attorneys into believing that confidentiality issues arise only through the vendor's practices.[129] Attorneys, however, have an affirmative duty to protect confidential information,[130] and those that do not consider what they can do to prevent disclosure on their side of the provider-attorney relationship are at risk of violating their professional obligations.[131]

In the circumstances precipitating the ethical opinion, the attorney came to the Committee seeking guidance on how to navigate the fog that spans between the attorney's ethical responsibilities and the cloud. The Committee, however, stated that this is a question "that the Lawyer must answer for himself,"[132] effectively throwing the ball back to the attorney.

The Massachusetts opinion is not unlike other opinions issued in that it missed a valuable opportunity to provide detailed guidance to attorneys. The opinions take the correct position that investigating cloud use requires due diligence, and, insofar as they can read to state, that attorneys themselves must conduct the investigation. Fortunately, provisions in Massachusetts state law give attorneys direct guidance on what issues to consider when evaluating ethical concerns that arise within the cloud.

IV. UPDATE IS READY: CONSUMER PROTECTION REGULATIONS THAT PROVIDE GUIDANCE AND A CLASSIFICATION SYSTEM THAT TAILORS

127. MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. 18 (2013), *available at* www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_6_confidentiality_of_information/comment_on_rule_1_6.html; MODEL RULES OF PROF'L CONDUCT R. 1.15 (2012).

128. Arguably, the committee provided one "reasonable effort" for daily use, which deals with monitoring the vendor's TUPP. Furthermore, the Committee also stated that attorneys should abide by their client's specific instruction on how their data should be stored and transmitted. *Id.* ¶ 8.

129. *See* BLACK, *supra* note 4, at 35 (stating that ethical issues are divided into two categories: vendor selection and daily use).

130. MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. 18 (2013), *available at* www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_6_confidentiality_of_information/comment_on_rule_1_6.html.

131. *Id.*

132. *Id.* ¶ 10.

SAFEGUARDS TO THE ATTORNEY'S USE

Attorneys seeking to understand more of the issues that are inherent with cloud computing can turn to the Massachusetts consumer protection regulations in order to obtain direct guidance on how to better comply with their ethical obligations. The Massachusetts law on protecting confidential information is one of the strictest in the nation and provides a valuable framework for analyzing one's policy on cloud computing.[133]

Additionally, attorneys can benefit from classifying their use of cloud computing within their own practice. This system allows attorneys to develop safeguards that are appropriate to the type of information stored within the cloud.

A. *Written Information Security Policy*

Massachusetts law requires every person that stores personal information to create, implement, and maintain a written information security policy ("WISP").[134] The purpose of the WISP is to ensure the security and confidentiality of clients' information.[135] The regulatory framework establishes minimum standards to safeguard personal information in order to guard against security threats and unauthorized access.[136]

The WISP regulations apply to all those that store, process, or maintain, either in writing or electronically, the personal information of a Massachusetts resident in connection with employment or the purchase of goods and services.[137] Personal information is defined as the resident's first and last name coupled with either the resident's social security number, driver's license number, or financial account number, including debit or credit card numbers.[138] As is evident from the breadth of residents covered by the regulation, few Massachusetts businesses and attorneys escape these comprehensive data security regulations.

The regulations create an affirmative duty to protect a client's personal information by detailing specific elements that the data holder's WISP should contain.[139] These elements include: ongoing training; policies to prevent terminated employees from accessing information; confirmation that a third party vendor will maintain the appropriate

133. *See* MASS. GEN. LAWS ch. 93H, § 2(c) (2012).

134. 201 MASS. CODE REGS. 17.03 (2012). A "person" includes, among others, natural persons and business entities. *Id.* § 17.02.

135. *Id.* § 17.01.

136. *Id.*

137. *Id.* § 17.02.

138. *Id.* (stating that the presence of the first initial satisfies the first name requirement).

139. *Id.* § 17.03.

security measures through an enforceable agreement; and an annual review of the WISP.[140]

A WISP must also cover a computer system's security.[141] The regulations dictate that the security policy must cover, among other things, passwords, system access, encryption, firewall protection, malware and anti-virus protection, and training.[142] The requirement of the encryption of personal information is one of the most significant protocols" and includes information stored on portable devices and personal information transmitted across public networks or wirelessly.[143]

While some may consider the Massachusetts WISP regulation as being onerous, for attorneys considering whether to enter the cloud computing marketplace, the WISP provides clearer guidance than the Committee's ethics opinion. Unlike the Committee's test, the WISP is not limited to vendor selection and it identifies in house concerns that the attorneys should address.[144]

The regulations, however, should not act as a complete deterrent for attorneys seeking to use cloud computing to aid their practice. The WISP regulation adopts a risk-based approach. In short, when implementing the organization's WISP, a business can take into account the size of the particular business, the scope of the business, the resources available, the nature and quantity of data stored, and the need for security.[145] In the end, Massachusetts's attorneys should consider both the Committee's test and the WISP regulations if they seek to store confidential information in the cloud, particularly personal information, as defined by the regulation.[146]

B. *A Cloud Classification System*

The classification system divides users into three separate categories: Class I, Class II, and Class III.[147] The user's category depends on what type of information the attorney stores in the cloud.[148]

140. *Id.*
141. 201 MASS. CODE REGS. 17.03 (2012).
142. *Id.* § 17.04.
143. *Id.*
144. *See supra* Part III.
145. MASS. GEN. LAWS ch. 93H, § 2(c) (2012).
146. 201 MASS. CODE REGS. 17.02 (2012).
147. The proposed classification system is based upon the document disposal system in Alabama. *See* Ala. State Bar Ethics Op. 2010-02, at 9-11 (2010). Furthermore, practicing attorneys have suggested that ethics committees encourage attorneys to assess the risks based on the appropriate level of use. *See* Letter from Carolyn Elefant, myShingle.com, to Alice Neece Mine, N.C. State Bar (Apr. 9, 2010) (on file with author).
148. *See* Ala. State Bar Ethics Op. 2010-02, at 9-11 (2010).

Each category contains safeguards that address the risks associated with the practitioner's use.

Class I users include attorneys that use cloud storage to maintain a library of forms or to store legal research.[149] The key characteristics of the data stored within this class are that the information stored does not need to be recorded and is not confidential. The baseline safeguard for a Class I user is a password policy.

In all IT security, a strong password is the first line of defense against breach.[150] In general, password security awareness is low[151] while hackers have grown more sophisticated.[152] Short passwords are easy to crack and must be replaced by passwords that are more complex[153] because complex passwords are more resistant to a hacker's attack.[154] Class I users should be concerned about password strength due to the potential need to guard confidential data that is stored inadvertently.

Furthermore, the policy should contain a password replacement procedure that establishes a regular interval of time after which users must change their passwords.[155] The interval creates a time limit during

149. *Cf.* Ala. State Bar Ethics Op. 2010-02, at 11 (2010) (stating that loss of this type of information would not result in an attorney breaching their duties). There are many services that are used daily that are cloud based. These services include Lexis, Westlaw, voicemail, text messaging, and online backup. *See* Letter from Legal Cloud Computing Association, to Alice Neece Mine, North Carolina State Bar (July 15, 2011) (on file with author), *available at* http://www.legalcloudcomputingassociation.org/Home/response-to-north-carolina-state-bar-proposed-2011feo6. Here, the critical distinction is between confidential and non-confidential. Nicole Black, *Proposed N.C. Bar Opinion Limits Cloud Computing*, NYLAWBLOG.TYPEPAD.COM, http://nylawblog.typepad.com/suigeneris/2011/06/north-carolina-bars-proposed-opinion-limits-lawyers-use-of-cloud-computing (last visited Apr. 14, 2015).

150. Chase, *supra* note 28, at 40.

151. A 2011 PC Magazine report found that among the top five passwords were 123456 and password. Passwords such as these are an invitation to breach. *See* NELSON ET AL., *supra* note 22, at 14.

152. Researchers have been able to design attacks, similar to those a hacker might use, that allow them to crack an eight-character password in less than two hours! *Id.*

153. A more complex password includes a mixture of numbers, symbols, and upper and lower case letters. *Id.*

154. Using techniques that cracked an eight-digit code in two hours, researchers estimate that it will take 17,134 years to crack a twelve-character password. *Id.*

155. A password security policy should also include procedures that the firm should take when an employee's employment ends because an ex-employee may be able to access data stored in the cloud and create security issues. *See* Pa. State Bar Comm. on Legal Ethics and Prof'l Responsibility, Formal Op. 2011-200, at 4 n.3 (2010) (discussing a fired employee who accessed content on cloud without authorization and deleted an entire upcoming season of a television series). Policies that prevent terminated employees from accessing personal information that is on record with a business are, in some cases, required by law. *See* 201 MASS. CODE REGS. 17.03(e) (2012).

which an unknown intruder can access the system.[156] Accordingly, a password policy that addresses both password strength and routine replacement will be an affirmative step that attorneys can take in order to protect against the inadvertent storage of a clients' confidential information,[157] and it will limit their exposure in the event of unauthorized access, thus providing a more competent storage of information.

Class II cloud storage users are attorneys that store documents and property that are related to the representation but are publicly available.[158] The common trait among these types of documents is that the attorney must preserve, record, or file them with the court.[159] Class II users store documents such as wills, powers of attorney, certificates of title, and official corporate records.[160] Building off the Class I safeguards, Class II users need to implement technologies, policies, and procedures that will allow them to meet their ethical responsibility of preserving the client's records.[161]

Data backup applies to Class II users because it will allow an attorney to obtain documents in the event that access to cloud storage is interrupted.[162] A backup, which is separate from the vendor's backup, can prove invaluable in the event that the cloud vendor collapses financially or if the attorney wants to terminate that vendor's service.[163] Without a separate backup, attorneys risk forfeiting all information stored on the vendor's server.[164]

156. A time limit can help to minimize damage. *See supra* text accompanying notes 57-8.

157. *See* Trope & Hughes, *supra* note 57, at 229; *see also Terms of Service,* CLIO, http://www.goclio.com/legal/tos/ (last visited Apr. 14, 2015) (stating that password security and password policies are the responsibility of the user).

158. *See cf.* Ala. State Bar Ethics Op. 2010-02, at 10 (2010) (stating that these types of documents need to be recorded, filed with the court, or given to the client).

159. *Id.*

160. *Id.* For illustrative purposes, other documents listed include advance directives, other executed estate planning documents, stock certificates, bonds, negotiable instruments, abstracts of title, deeds, and settlement agreements. *Id.*

161. MODEL RULES OF PROF'L CONDUCT R. 1.15 (2012), *available at* http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_15_safekeeping_property.html.

162. Ala. State Bar Ethics Op. 2010-02, at 11, 13 (2010) (stating that documents of this nature must be preserved indefinitely and that a lawyer "must 'back up' all electronically stored files").

163. *See* NELSON ET AL., *supra* note 22, at 107-111.

164. It is important to note that an additional backup does not require a cloud-using attorney to do more than a traditional attorney. Attorneys that do not use cloud storage, generally, save a document on their computer, print one for the file, and send a copy out. With a backup requirement, cloud attorneys will store one in the cloud, one in their backup,

"Access to Data Agreements" with the vendor is another safeguard of this Class.[165] These agreements allow attorneys to access the files stored with the vendor so that they can download and reproduce them in a non-proprietary format[166] in the event of a change of cloud vendors, by client request, and even if the attorney is retiring and needs to turn to documents over to the court or the client.[167] Firms that implement safeguards that address data loss and data reproduction will inevitably provide a higher level of compliance to the obligation to safeguard the client's property because they will have multiple methods to access the client's stored information.[168]

Finally, Class III users utilize cloud storage for confidential client information.[169] Examples of Class III users include attorneys that use the cloud to store intangible personal property, discovery, written statements, photographs, and recordings.[170] Due to the confidential nature of the information stored by a Class III user, the highest levels of security should be the standard.

Attorneys should consider security concerns in both selecting a vendor and in their daily use.[171] Cloud vendors have set forth a list of what they consider to be "minimal standards" that provide a "baseline of security and privacy guarantees," and this list provides a solid foundation for establishing what technical specifications the vendor and the user should be able to comply with.[172] This list, coupled with the

and send one copy out. Therefore, this requirement allows attorneys to safeguard the client's property without additional procedural burdens.

165. Bob Ambrogi, *N.C. Ethics Opinion on SaaS Merits Broader Inquiry*, CATALYSTSECURE.COM, http://www.catalystsecure.com/blog/2010/05/n-c-ethics-opinion-on-saas-merits-broader-inquiry/ (last visited on Apr. 14, 2015).

166. Letter from Jack Newton et al., LCCA, to Natalia Vera, ABA Center of Professional Responsibility (Dec. 15, 2010) (on file with author).

167. Ala. State Bar Ethics Op. 2010-02, at 16 (2010) (stating that whatever format attorneys choose to store client documents, they must be able to reproduce the document in its original paper format).

168. MODEL RULES OF PROF'L CONDUCT R. 1.15 (2012), *available at* http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_15_safekeeping_property.html; *see* Ala. State Bar Ethics Op. 2010-02, at 11, 13 (2010) (stating that documents of this nature must be preserved indefinitely).

169. Ala. State Bar Ethics Op. 2010-02, at 10-11 (2010) (describing the category as information the attorney has that is specifically related the representation and may be considered confidential).

170. *Id.* This category include pleadings, correspondence, demonstrative aids, notes, memoranda, and voluminous financial, accounting, or business records. *Id.*

171. BLACK, *supra* note 4, at 35.

172. Newton et al., *supra* note 166 (outlining minimal standards for secure data centers, network security, software security, data transmission security, backups and redundancy, confidentiality and privacy, and data portability). These standards include cloud server

vendor test provided by the Massachusetts Committee and the issues raised by the Pennsylvania ethics opinion, allow Massachusetts attorneys to create a basic understanding of the concerns they need to address when they are seeking a cloud vendor.[173] Like in New Jersey or the WISP, attorneys should also look to have an enforceable agreement with the cloud vendor that stores confidential information.

Cloud computing does not stop at the selection of the vendor. Class III users must address security concerns that arise from their daily use of cloud storage.[174] In addition to the Class I and Class II safeguards, the Class III user, like a WISP, needs to address issues such as system access, encryption, firewall protection, malware and anti-virus protection, and training.[175]

Obtaining a client's consent before storing confidential information in the cloud is another issue that Class III users should consider.[176] Informed consent exists when the attorney fully advises the client about

security audits, guarantees of confidentiality, and availability of information for attorneys to download. *Id.* Downloading includes all "mission critical" information and the information should be put into a non-proprietary format. *Id.*

173. Pa. State Bar Comm. on Legal Ethics and Prof'l Responsibility, Formal Op. 2011-200, at 4 n.3 (2010). For example, other requirements for vendor selection include lost data procedures, data ownership resolution, the vendor's server location, and questions of liability. *Id.*; *see also* State Bar N.C., 2011 Formal Ethics Op. 6, ¶ 14 (2012) (proposing a list of recommended security inquires). An organization, like LCCA, *see supra* note 29, should be asked to provide an updated list of minimal standards in order to remain current with changes in technology. Additionally, some attorneys would like their state bars to provide a list of "certified" vendors. *See* Email from Christopher Fulmer, Attorney, to Alice Mine, N.C. State Bar (Apr. 7, 2010, 10:44 EST) (on file with author).

174. This policy should provide guidelines for establishing complex passwords, routine password changes, and procedures for certain events, such as a terminated employee.

175. 201 MASS. CODE REGS. 17.04 (2012); *see* State Bar N.C., 2011 Formal Ethics Op. 6, ¶ 5 (2012) (ongoing training requirement). Attorneys should encourage their state and local bars to provide adequate training opportunities and resources their members. *See generally Questions to Ask Cloud Providers*, SCBAR.ORG, http://www.scbar.org/public/files/docs/VendorQ.pdf (last visited Apr. 14, 2015) (providing a list of questions attorneys can consider when investigating the cloud). The MRPC state that staying abreast of relevant technology is a part of maintaining competence. MODEL RULES OF PROF'L CONDUCT R. 1.1 cmt. 8 (2013), *available at* www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_1_competence/comment_on_rule_1_1.html. Education and training can prevent security breaches. *See* State Bar N.C., 2011 Formal Ethics Op. 6, ¶ 5 (2012); Ala. State Bar Ethics Op. 2010-02, at 16 (2010). The LCCA, *see supra* note 29, recommends the creation of an educational resource for attorneys with features including best practices, an overview of terms and concepts, articles on new developments, and links to other bar associations websites. Newton et al., *supra* 166.

176. *See* Trope & Hughes, *supra* note 57, at 229; *see also* Ala. State Bar Ethics Op. 2010-02, at 10 (2010) (stating that the destruction of client documents in this category requires consent). Furthermore, Alabama requires attorneys to have a file retention policy and, at the outset of the representation, the attorney must communicate the policy in writing to the client. *Id.* at 5.

the nature, purpose, benefits, and detriments that may result from an action.[177] Such consent, as it relates to cloud storage, has the potential to both improve the attorney's awareness of security risks and to better protect the client's confidential information.

While attorneys may not be comfortable with addressing cloud storage with a client or may believe that the client expects the attorney to store data electronically, relying on a sort of implied consent is dangerous to the attorney.[178] The obligation of securing confidential information extends to all parties involved with the attorney, including cloud vendors.[179] Attorneys may share a client's confidential information within the firm, but sharing "does not extend to outside entities or to individuals over whom the firm lacks effective supervision and control."[180] By using a cloud vendor, the attorney is outsourcing because the vendor is responsible for the data storage. As a result, it would be prudent for an attorney to not only inform the client of the firm's use of cloud storage, but to have the client consent to the disclosure.[181]

Informed consent can provide for representation that is more competent. In order to inform the client about the use, purpose, and risks of using the cloud,[182] the attorneys themselves will need to have a working knowledge of these issues. The level of knowledge needed to articulate, even in the most general way, how their cloud storage works, the practices their office uses, the general practices of cloud use, and the security measures needed to guard against intrusion will aid attorneys in meeting the competency standards of representation.[183]

Additionally, Rule 1.6 requires that attorneys exercise reasonable, affirmative steps to protect against the risk of inadvertent disclosure of the client's confidential information.[184] This obligation extends to all

177. State Bar Cal. Standing Comm. on Prof'l Responsibility and Conduct, Formal Op. 2010-179, at 5 n.15 (2010). Cloud computing transmits information over the internet each time a documents are uploaded or downloaded to the cloud based program.

178. Trope & Hughes, *supra* note 57, at 228.

179. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 08-451 (2008) (discussing a lawyers obligations when outsourcing both legal and non-legal services).

180. *Id.*

181. MODEL RULES OF PROF'L CONDUCT R. 1.6 (2012). In Massachusetts, one must abide by a client's order not to store data in the cloud. Presumably, clients must have some level of knowledge before they can reject the use of cloud storage. Mass. State Bar Comm. on Prof'l Responsibility, Formal Op. 12-03 (2012).

182. *See supra* Part I.D.

183. MODEL RULES OF PROF'L CONDUCT R. 1.1 (2012). "Competent representation requires the legal knowledge, skill, thoroughness, and preparation reasonably necessary for the representation." *Id.*

184. Trope & Hughes, *supra* note 57, at 229.

who are "participating in the representation."[185] A consent requirement will help to create a greater need to investigate a cloud vendor and will aid attorneys in meeting the "reasonable efforts" test required by the Massachusetts Committee.[186]

In sum, the classification system helps to narrow the issues that need to be addressed. Attorneys that categorize their use will be able to investigate cloud technology as it relates to their needs, thereby allowing them to hone in on the specific actions that they must take in order to meet their ethical obligations of competency, confidentiality, and the safeguarding of property.[187] For example, a new transactional attorney who wants to store legal forms in the cloud will not be bogged down by having to investigate the security audit process of their cloud host.[188]

Furthermore, the classification system helps to eliminate some of the assumptions that are inherent with arguments for and against the reasonableness standard as applied to cloud computing. To demonstrate, opponents of mandatory requirements argue that such requirements assume that all attorneys are storing confidential information in the cloud.[189] Confining confidential use to its own category, however, quickly dismantles this argument. On the other side, the reasonableness standard assumes that attorneys know what the risks of cloud computing are, or that an outside professional can provide guidance on how to apply the attorney's professional responsibilities to the technical aspects of cloud storage.[190] The cloud industry, however, does not believe that attorneys understand the risks that lay within the cloud,[191] and obtaining an unbiased IT professional's opinion may be a challenge because, without server and maintenance needs, the cloud itself is a threat to their business model. This gives attorneys limited places to turn in order to seek constructive guidance on how to meet their ethical obligations. By

185. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 08-451 (2008) (discussing Rule 1.6, comment 5 and a lawyer's obligations when outsourcing both legal and non-legal services).

186. Mass. State Bar Comm. on Prof'l Responsibility, Formal Op. 12-03 (2012).

187. The issue presented to each ethics committee can vary and as a result, the opinions can yield a different level of guidance under the reasonableness standard. *Compare* State Bar N.C., 2011 Formal Ethics Op. 6, ¶ 3 (2012) (presenting the issue of "may a law firm use SaaS?"), *with* State Bar of Ariz. Formal Ethics Op. 09-04, ¶ 3 (2009) (dealing with the issue of an encrypted online file and retrieval system where each document was password protected and coded in an alpha numeric system).

188. This attorney is a Class I user and the audit would fall under Class III. *See generally* Newton et al., *supra* note 166 (stating the audit is a minimal requirement).

189. *See* Black, *supra* note 149.

190. *Id.*

191. *See* Newton et al., *supra* note 166 (stating that cloud vendors "do not believe presently, that most lawyers . . . have a sufficient understanding of [web-based technologies], and the risks associated with those technologies.").

narrowing cloud storage into categories, attorneys should be hopeful that *legal* professionals (attorneys, state and local bars, and ethics committees) will be able to help them to identify the inherent risks and adopt specific measures that allow those attorneys to meet their professional obligations.

CONCLUSION

The legal profession has a tendency to cling to the past and make decisions concerning technology that will hamper the profession in the long term.[192] Attorneys "revere precedent and distrust change."[193] This is a mistake when dealing with the use of cloud computing[194] and the standards set forth for its use.

The profession clearly recognizes there is sufficient room in the cloud for efficiencies, cost savings, and ethical compliance. Most of the ethics opinions, however, are vague due to the nature of the technology and its youth. Attorneys conducting their investigation into the use of the cloud must also consider sources beyond the ethics opinions because, generally, the one-size-fits-all reasonable care standard fails to provide adequate guidance. Consumer protection statutes and the user classification system, with its class specific safeguards, offer direct guidance on how attorneys can comply with their ethical obligations while obtaining the benefits of the cloud.

In the legal profession, cloud computing is in its infancy. As we press on in the new century of technology, secure and competent data storage will not only protect the client's property and confidentiality, but it will protect the reputation of the cloud computing attorney and the legal profession as a whole.

192. BLACK, *supra* note 4, at 148.
193. *Id.*
194. *Id.*