McGeorge Law Review

Volume 45 | Issue 4 Article 8

1-1-2014

Seeing Clearly? Interpreting Model Rule 1.6(c) for Attorney Use of Cloud Computing Technology

Myles G. Taylor
Pacific McGeorge School of Law

Seeing Clearly? Interpreting Model Rule 1.6(c) for Attorney Use of Cloud Computing Technology

Myles G. Taylor*

TABLE OF CONTENTS

I. INTRODUCTION

When it comes to familiarity with cutting-edge technology, attorneys are a diverse group. Some attorneys are troubled by the use of new technologies and try to avoid it.[1] At the same time, many attorneys not only embrace but also

* J.D., University of the Pacific, McGeorge School of Law, 2014; B.A., University of California, Davis, 2011. Many thanks to Mark Freeman, Andrew Hsieh, Chris Blau, Danielle Lenth, Professor Fred Galves, and the members and editors of the *McGeorge Law Review* for assistance in writing this Comment.

1. *See, e.g.*, *J.D. as I.T.*, THE NAMBY PAMBY (May 24, 2012), http://thenambypambyblog.com/2012/05/24/j-d-as-i-t/ (on file with the *McGeorge Law Review*). Popular blogger and attorney, "The Namby Pamby,"

enthusiastically support new technologies that benefit the practice of law.[2] Beginning in the mid-2000s, attorneys following the budding trends of new computing technology began to notice a gap between what was merely best practices for safekeeping of data and what was ethically required.[3] Cloud computing, which involves computing "services . . . controlled by third-parties and access[ed] over the Internet," was one emerging technology that widened this gap.[4]

Although it was not the first new technology to do so, cloud computing raised numerous ethical issues when the legal community began to explore its possibilities.[5] Significantly, the use of cloud computing raised issues with the attorney's duty of confidentiality due to its defining characteristics.[6] Attorneys faced uncertainty over the ethical use of cloud computing because of the lack of practical guidance available.[7] In response to this issue and others, the American Bar Association established the ABA Commission on Ethics 20/20 ("the Commission"), which, after several draft proposals, developed a new round of amendments to the Model Rules.[8] The most significant amendment relating to cloud computing was Model Rule 1.6(c), which added an affirmative prevention requirement to the duty of client confidentiality.[9]

---

has written about this from personal experience. On one occasion, he documented a phone call with a partner at his firm:

> Partner: What are you doing?
>
> Me: Writing a brief. Can I help you with something?
>
> Partner: I need you to help me get something out of the trashcan.
>
> Me: Uh . . . Your actual trashcan or the one on your computer screen.
>
> Partner: Uh . . . the computer one.
>
> Me: I'll be right there. *Id.*

2. *See* Richard M. Goehler et al., *Technology Traps: Ethical Considerations for Litigators in a 24/7 Online World*, 36 LITIGATION 34 (2010) ("Many attorneys believe that to compete in the legal marketplace, they must master the new ways in which individuals use technology to communicate.").

3. ABA COMM'N ON ETHICS 20/20, ISSUES PAPER CONCERNING CLIENT CONFIDENTIALITY AND LAWYERS USE OF TECHNOLOGY 2 (2010), *available at* http://www.americanbar.org/content/dam/aba/migrated/2011_build/ethics_2020/clientconfidentiality_issuespaper.pdf [hereinafter COMMISSION ISSUES PAPER] (on file with the *McGeorge Law Review*).

4. *Id.*

5. *See, e.g.*, ABA Comm'n on Ethics & Prof'l Responsibility, Formal Op. 99-413 (1999) (determining attorneys may transmit confidential information by unencrypted email without violating the Model Rules).

6. *See infra* Part III (discussing the development of Model Rule 1.6(c)).

7. Since the obligations under the Model Rules did not address it, many state bar associations attempted to issue their own opinions on the use of cloud computing. *See, e.g.*, Pa. Bar Ass'n Comm. Legal Ethics & Prof'l Responsibility, Formal Op. 2011-200 (2011) (determining Pennsylvania ethical obligations for attorneys using cloud computing and confidentiality).

8. ABA COMM'N ON ETHICS 20/20, RESOLUTION TO HOUSE OF DELEGATES 4–5 (2012), *available at* http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/20120508_ethics_20_20_final_resolution_and_report_technology_and_confidentiality_posting.authcheckdam.pdf [hereinafter COMMISSION RESOLUTION] (on file with the *McGeorge Law Review*).

9. *Id.*

This Comment approaches Model Rule 1.6(c) from the perspective of an attorney using cloud computing services and argues that, while the rule's current iteration succeeds as a general rule clarifying the existence of an affirmative safeguard obligation, it fails to provide real instruction and guidance to attorneys in practice who are seeking to meet their ethical obligations. Part II of this Comment evaluates cloud computing services and concludes that, despite the risks, attorneys benefit greatly from incorporating cloud computing into their practices as long as they meet their ethical duties. Part III then explains the duty of client confidentiality and the need for a rule addressing new technology uses. Part IV analyzes the goals of Model Rule 1.6(c) as both a practical guide and as an ethical clarification to determine whether it achieves its original purposes. Next, this Comment argues that the rule, as interpreted by the factors in its official comment, fails to adequately meet its goals. Finally, it proposes a solution to address the identified shortcomings.

II. CLOUD COMPUTING AND THE PRACTICE OF LAW

Attorneys, like other professionals, incorporate new technology into their practices when it serves their needs. However, due to the unique responsibilities of the legal profession,[10] attorneys must evaluate any technology's impact on their ethical obligations before jumping on the bandwagon.[11]

A. Explanation of Cloud Computing

Cloud computing refers "to services that are controlled by third-parties and accessed over the Internet."[12] Unlike traditional forms of computing, which

10. *See generally* MODEL RULES OF PROF'L CONDUCT (2012) (serving as the model for most jurisdiction's ethics rules).

11. Small business owners that do not face the same ethical obligations as attorneys have less to worry about when adopting cloud computing services. *Cf.* Marcy Hoffman, *Is the Cloud Secure Enough for Your Small Business?*, INFOSTREET'S SMALL BUSINESS BLOG (Aug. 22, 2012), http://smallbusinessblog.infostreet.com/2012/08/is-the-cloud-secure-enough-for-your-small-business/ (on file with the *McGeorge Law Review*) (discussing security needs for small business, which can differ from a law practice); Jesse Lipson, *Is Your Data Safe in the Cloud?*, FORBES (Mar. 16, 2011, 1:56 PM), http://www.forbes.com/sites/ciocentral/2011/03/16/is-your-data-safe-in-the-cloud/ (on file with the *McGeorge Law Review*) (claiming that safety concerns are a result of "your brain . . . conflating control with safety").

12. COMMISSION ISSUES PAPER, *supra* note 3, at 1. This simple and likely flawed definition can be compared with the more detailed definition given by the National Institute of Standards and Technology (NIST), a division of the US Department of Commerce, which declares: "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources . . . that can be rapidly provisioned and released with minimal management effort or service provider interaction." NAT'L INST. STANDARDS & TECH., SPECIAL PUBLICATION 800-146, CLOUD COMPUTING SYNOPSIS AND RECOMMENDATIONS 2-1 (2012), *available at* http://csrc.nist.gov/publications/nistpubs/800-146/sp800-146.pdf [hereinafter NIST] (on file with the *McGeorge Law Review*). The five essential characteristics of a cloud computing service are identified by the NIST as on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. *Id.*

require the user to install software or store data locally, cloud computing companies allow the user to access services and data through any compatible Internet connected device.[13] Many forms of cloud computing exist, but the most common types that attorneys will encounter are online storage and backup,[14] web-based email,[15] and software-as-a-service, which "replace[s] costly licensed software with purportedly less expensive access to software on an as needed basis."[16] In addition to general use services, some cloud software suites are made specifically for law practice management.[17] These low-cost, web-based solutions have even made it possible for attorneys to operate "virtual law offices," which gives attorneys the ability to practice without a traditional office.[18]

B. Risks for Attorneys

All users of cloud computing services encounter a host of risks, but due to heightened ethical responsibilities in the legal profession, attorneys face potentially greater ones.[19] The ABA Commission outlined a list of risks related specifically to the attorney's duty of confidentiality when using cloud computing services.[20] These risks focus on the fear of digital theft and hacking, loss of data, and inadvertent disclosure of sensitive information.[21] Commentators have also found a number of risks associated with the lack of control over the software or data when using cloud computing.[22]

The Commission acknowledged that theft of information can occur because of malicious, intentional security breaches.[23] Hackers find little difference

13. NIST, *supra* note 12, at 2-1, 2-2.

14. Storage and backup includes popular services such as Dropbox (http://dropbox.com), Mozy (http://mozy.com), and Carbonite (http://carbonite.com). Online storage functions as a separate drive that allows for easy access, while online backup protects more in the event of data loss.

15. Mark Brownlow, *Email and Webmail Statistics*, EMAIL MARKETING REPORTS (Dec. 2012), http://www.email-marketing-reports.com/metrics/email-statistics.htm (on file with the *McGeorge Law Review*). The three main providers of web-based email (Microsoft's Hotmail, Yahoo! Mail, and Gmail) total well over one billion users. *Id.*

16. 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, 169 (2011).

17. Clio, for example, provides cloud-based calendaring, time tracking, note-taking, document management, trust accounting, managing retainers, and billing all within the same service. CLIO, http://www.goclio.com (last visited Mar. 19, 2014) (on file with the *McGeorge Law Review*).

18. In a 2011 non-binding formal opinion, the California State Bar acknowledged this new trend and concluded that virtual law office practitioners have no "greater or different [ethical] duties" than those practicing in a traditional law office. Cal. State Bar Comm'n Prof'l Responsibility, Ethics Op. 2010-0003 (2010).

19. *See generally* MODEL RULES OF PROF'L CONDUCT (2012) (serving as the model for ethics rules of most states).

20. COMMISSION ISSUES PAPER, *supra* note 3, at 2.

21. *Id.*

22. Trope & Hughes, *supra* note 16.

23. COMMISSION ISSUES PAPER, *supra* note 3, at 2.

between cloud and non-cloud services and will attempt to break into anything worthwhile.[24] For example, technology journalist Mat Honan lost his entire digital life due to a flaw in the information used to verify identity across services.[25] In another case, electronics manufacturer Sony faced a large-scale attack when hackers utilized Amazon's cloud-based servers as weapons to shut down the Japanese company's online services.[26] Although some companies hold a reputation for optimal digital security,[27] there will always be a risk associated with malicious and intentional data disclosure.[28]

Attorneys should be aware of the many other risks involved with using cloud computing services. Beyond issues of outsiders breaking in, risks can arise from user error or accidental disclosure of information by the provider.[29] These risks include decreased control over and decreased knowledge of the software and its potential instabilities,[30] the security features used to protect the information,[31] the existence of data breaches,[32] and the location of the storage.[33] Further, there are

24. Kevin Fogarty, *The Biggest Cloud Computing Security Risk Is Impossible to Eliminate*, NETWORK COMPUTING (Aug. 10, 2012), http://www.networkcomputing.com/security/the-biggest-cloud-computing-security-ris/240005337 (on file with the *McGeorge Law Review*) ("Except for the potential booty (money, data or notoriety), cloud and non-cloud services look pretty much the same to criminals trying to crack them open.").

25. *See* Mat Honan, *How Apple and Amazon Security Flaws Led to My Epic Hacking*, WIRED (Aug. 6, 2012, 8:01 PM), http://www.wired.com/gadgetlab/2012/08/apple-amazon-mat-honan-hacking/ (on file with the *McGeorge Law Review*). Mat Honan summarizes how the hacking occurred:

> In short, the very four digits that Amazon considers unimportant enough to display in the clear on the web are precisely the same ones that Apple considers secure enough to perform identity verification. The disconnect exposes flaws in data management policies endemic to the entire technology industry, and points to a looming nightmare as we enter the era of cloud computing and connected devices. *Id.*

26. Joseph Galante, Olga Kharif & Pavel Alpeyev, *Sony Network Breach Shows Amazon Cloud's Appeal for Hackers*, BLOOMBERG NEWS (May 16, 2011, 1:45 PM), http://www.bloomberg.com/news/2011-05-15/sony-attack-shows-amazon-s-cloud-service-lures-hackers-at-pennies-an-hour.html (on file with the *McGeorge Law Review*).

27. E-discovery company Catalyst, for example, has been vetted by and hosted repositories for "banks, major software companies, insurers and the U.S. government for sensitive terrorist materials." *Why Catalyst for Complex E-Discovery*, CATALYST, http://www.catalystsecure.com/about/why-catalyst/key-benefits.html (last visited Jan. 7, 2014) (on file with the *McGeorge Law Review*).

28. *See, e.g.*, Natasha Lennard, *Anonymous Hacks U.S. Sentencing Commission Website for Aaron Swartz*, SALON (Jan. 28, 2013, 6:30 AM), http://www.salon.com/2013/01/28/anonymous_hacks_doj_website_for_aaron_swartz/ (on file with the *McGeorge Law Review*) (explaining the motivation for multiple successful attempts at hacking of the US Sentencing Commission website during January 2013).

29. *See generally* Trope & Hughes, *supra* note 16 (discussing the risks of cloud computing for attorneys in-depth); Audrey Watters, *Google's Internal Security Breach Raises Questions About Trust and the Cloud*, READWRITEWEB (Sept. 16, 2010), http://www.readwriteweb.com/cloud/2010/09/googles-internal-security-brea (on file with the *McGeorge Law Review*) (discussing an internal security breach at Google by an employee). *But see* Larry Walsh, *Red Herrings in Cloud Computing*, CHANNELNOMICS (Sept. 17, 2010), http://channelnomics.com/2010/09/17/red-herrings-in-cloud-computing/ (on file with the *McGeorge Law Review*) (rebutting the safety concerns over Google's cloud services).

30. Trope & Hughes, *supra* note 16, at 175. Diminished control can be especially problematic if there are crashes or outages that could leave an attorney without access to his or her data. *Id.*

31. *Id.* at 215–16.

32. *Id.* at 218–19.

also risks of government surveillance or seizure.[34] These risks are inherent when allowing someone else to have complete control over one's data. In fact, Steve Wozniak, co-founder of Apple, warns that the over-reliance on cloud services is "going to be horrendous" and predicts "a lot of horrible problems" as a result of this lack of control.[35] If a server goes down on the provider's side, for example, attorneys can lose access to client information and may be unable to retrieve it.[36]

C. Benefits for Attorneys

Cloud computing does bear significant risks; however, this is true for all technologies. While a candid review of cloud computing discloses a list of potential issues, there are significant benefits for attorneys. Attorneys benefit from cloud computing because these services grant greater accessibility to information, provide the same or better services as locally stored data at lower cost, and improve efficiency by simplifying the user experience with easy web-based access.[37]

First, attorneys have more access to their data when using cloud computing services because it can be made easily available from many locations and on many devices.[38] Attorneys can utilize the "linkage and integration of the numerous computing devices" to connect with their work more quickly and easily.[39] This saves time and brings costs down by streamlining attorneys' access to their information.

Second, cloud computing services are generally much cheaper than traditional options because sharing physical computing resources, including networking and storage, helps to distribute expenses to keep costs down over a

33. *Id.* at 224–26.

34. *Id.* at 230–33. This area has become particularly fertile due to recent revelations about the extent of the National Security Agency's surveillance programs. *See NSA Spying on Americans*, ELECTRONIC FRONTIER FOUNDATION, http://www.eff.org/nsa-spying (last visited March 16, 2014) (on file with the *McGeorge Law Review*) (collecting revelations and updates on the issue); *see also* Letter from James R. Silkenat, President, American Bar Association, to General Keith B. Alexander, Director, National Security Agency (February 20, 2014) (on file with the *McGeorge Law Review*) (expressing concerns over the surveillance of American lawyers' confidential communications with overseas clients).

35. Shane Richmond, *Apple Founder Warns of 'Horrendous' Cloud Computing Risks*, TELEGRAPH (Aug. 6, 2012, 3:11 PM), http://www.telegraph.co.uk/technology/apple/9456281/Apple-founder-warns-of-horrendous-cloud-computing-risks.html (on file with the *McGeorge Law Review*).

36. This issue has caused some attorneys to question the benefits of cloud storage. One attorney wrote on his blog that "[p]erhaps [the] old guy who never got a computer and gets his secretary to print all his emails for him to read has it right after all." Phillip W. Thomas, *Amazon Crash Has Me Re-thinking the Cloud*, MS LITIG. REV. AND COMMENTARY (Oct. 25, 2012), http://www.mslitigationreview.com/2012/10/articles/general-1/amazon-crash-has-me-rethinking-the-cloud/ (on file with the *McGeorge Law Review*).

37. *See* Shellie Stephens, *Going Google: Your Practice, The Cloud, and the ABA Commission on Ethics 20/20*, 2011 U. ILL. J. L. TECH. & POL'Y 237, 238–39 (2011) (discussing benefits of cloud computing for lawyers).

38. Trope & Hughes, *supra* note 16, at 168.

39. *Id.*

larger user base.[40] Attorneys can reduce startup and maintenance costs by using cloud services instead of utilizing more expensive traditional hardware and software.[41] Attorneys also save money from the reduced need for IT personnel, as there is less to administer on the user's end.[42]

Finally, attorneys benefit from the efficiency of cloud computing services. Cloud services often present a seamless user interface, keeping most technical aspects hidden.[43] When there is a problem, the service provider can find a solution without the need for the user to download and install updates locally.[44] Because data and programs are stored off-site, attorneys do not risk losing important information to accidents like computer malfunction, fire, or other property damage at their offices.[45] Attorneys seeking to optimize their practices by "going paperless" also benefit vastly from the gains of cloud services over using an in house system, especially for those attorneys without vast resources to spend on overhead costs.[46]

D. Evaluation of Cloud Computing Use

Although some hold doubts about its use, cloud computing is generally secure enough for attorneys to use without worrying that the sky is falling.[47] This is especially true when compared to the alternatives of physical documents or locally stored electronic data.[48] A client file that exists in physical form or electronically on a local drive could be destroyed, stolen, or misplaced in the

40. Shannon Brown, *Navigating the Fog of Cloud Computing*, 33 PA. LAW. 19 (2011).

41. At the time of this Comment, Google offers 15 GB of storage for free to all users. *Storage Plan Pricing*, GOOGLE.COM, https://support.google.com/drive/answer/2375123?hl=en&p=mktg_pricing (last visited Jan. 7, 2014) (on file with the *McGeorge Law Review*); *see also* Shawn L. Holahan, *Silver Lining in That Cloud*, 60 LA. B.J. 320 (2013) ("In essence, law firms rent software through the cloud instead of purchasing it. . . .").

42. Trope & Hughes, *supra* note 16, at 166 ("Potential clients are being encouraged to scrap their in-house servers and save on the associated costs by outsourcing their data storage and processing to off-premises server farms . . . .").

43. The popular attorney cloud service, Clio, is a good example of a service that presents the end user with a simple, intuitive format. CLIO, http://www.goclio.com/ (last visited Mar. 19, 2014) (on file with the *McGeorge Law Review*).

44. NIST, *supra* note 12, at 2-1, 2-2.

45. It is possible that these accidents could take place at the cloud server location; however, because cloud service providers are in the business of holding data, it is reasonable to find that data stored by professionals is less susceptible to such accidents than that stored by an end-user. *See, e.g.*, Lipson, *supra* note 11 ("Cloud software companies, knowing the implications of a crash on their business' bottom line, invest significant resources into insuring that such a disaster never occurs. Cloud computing companies can invest far more resources in data backup and security than your business can.").

46. Laura A. Calloway, *How to Go Paperless*, 39 LAW PRACTICE 12 (2003).

47. *Cf.* Kenneth L. Bostick, Comment, *Pie in the Sky: Cloud Computing Brings an End to the Professionalism Paradigm in the Practice of Law*, 60 BUFF. L. REV. 1375, 1414–15 (2012) (arguing that cloud computing "challenge[s the] ideology of the practice of law as an autonomous profession" and promotes a "business of law" mentality).

48. *See, e.g.*, Hoffman, *supra* note 11 (comparing the full-time resources of a cloud computing company to "the levels of protection that [a] part-time IT person provides").

same way that a file stored on a third-party cloud server could.[49] Further, information stored on an internet-connected local server or personal computer is vulnerable to attack or error even with safeguards in place; yet with cloud services, the company is likely to monitor and employ state-of-the-art protections as their business depends on providing as safe and high-quality a service as is practicable.[50] As one commentator stated, the fear of using cloud computing is the "same fallacy [that] causes some people to be afraid of flying on an airplane."[51] Since data stored in an encrypted form on remote servers is at least as secure as more traditional electronic means of storing client information, attorneys should generally welcome cloud computing as a significant benefit to their practices.

Yet acknowledging that cloud computing is generally safe for use is only the first step. Attorneys must be fully aware of the ethical obligations that are implicated before signing up. Inherently, users of cloud services must accept the fact that another is in control of the user's data and that the user has less knowledge of the services' operations when compared with traditional, in-house solutions.[52] Attorneys implicate the duty of confidentiality when others have access to or control over sensitive client information because the attorney is ultimately responsible for ensuring that confidentiality is maintained.[53] Thus, attorneys ought to understand their responsibilities under the duty of confidentiality before they utilize a tool that could potentially lead to a breach.[54]

III. THE DUTY OF CONFIDENTIALITY AND MODEL RULE 1.6(C)

Attorneys are governed by specific ethical rules, and while these rules differ depending on the jurisdiction, the duty of confidentiality is a bedrock doctrine across the profession. It is not always clear, however, how changes to technology impact this ethical obligation.

49. *See* COMMISSION ISSUES PAPER, *supra* note 3, at 2 ("The Commission's efforts have been guided by the reality that information, whether in electronic or physical form, is susceptible to theft, loss, or inadvertent disclosure.").

50. Clio, for instance, boasts "security and privacy of your data are our top priority" and presents information about its encryption, privacy policy, and daily auditing, which "help[s] ensure your data is protected from security vulnerabilities and other online threats." *Security*, CLIO, http://app.goclio.com/security (last visited Mar. 19, 2014) (on file with the *McGeorge Law Review*).

51. Lipson, *supra* note 11.

52. *See* Richmond, *supra* note 35 ("I say the more we transfer everything onto the web, onto the cloud, the less we're going to have control over it.")

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

54. Of course, cloud computing is not unique to confidentiality issues. For purposes of this Comment, however, the discussion is limited.

A. Ethical Conduct Under the Model Rules

Attorneys are subject to many rules that govern professional ethics.[55] The ABA publishes the Model Rules of Professional Conduct to provide "leadership in legal ethics and professional responsibility through the adoption of professional standards that serve as models of the regulatory law governing the legal profession."[56] Like the Model Penal Code for criminal law,[57] the Model Rules of Professional Conduct are not binding unless enacted by jurisdictions with enforcement power.[58] Excluding California, all jurisdictions in the United States follow some form of the Model Rules.[59]

Whether or not the Model Rules are adopted directly, all forms of ethics rules have distinctly shaped how attorneys are expected to practice. Violations of these rules can result in disciplinary consequences that range from additional ethics training to disbarment.[60] Each state bar has some form of disciplinary branch to address these violations.[61] And although the Model Rules are not meant as a basis for civil liability,[62] courts have admitted violations as evidence of professional malpractice in private causes of action.[63]

B. The Duty of Confidentiality

Model Rule 1.6(a) lays out the attorney's ethical duty of confidentiality:[64]

> A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is

55. *See generally* MODEL RULES OF PROF'L CONDUCT (2012).

56. *Id.* at Preface.

57. *See generally* MODEL PENAL CODE (1962).

58. These jurisdictions include all fifty states, the District of Columbia, and the Virgin Islands. *Alphabetical List of States Adopting Model Rules*, AM. BAR ASS'N CTR. FOR PROF'L RESPONSIBILITY, http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/alpha_list_state_adopting_model_rules.html (last visited Jan. 14, 2013) (on file with the *McGeorge Law Review*).

59. *Id.*

60. MODEL RULES PROF'L CONDUCT pmbl. cmt. 19 (2012).

61. *Directory of Lawyer Disciplinary Agencies 2011–12*, ABA, http://www.americanbar.org/content/dam/aba/migrated/cpr/regulation/directory.authcheckdam.pdf (last visited Feb. 22, 2014) (on file with the *McGeorge Law Review*).

62. MODEL RULES PROF'L CONDUCT pmbl. 20 (2012).

63. *See* Gena L. Sluga & Douglas L. Christian, *Playing by the Rules: Violations of Ethics Rules as Evidence of Legal Malpractice*, 51 FED'N DEF. AND CORP. COUNS. Q., 6 (2001), *available at* http://www.thefederation.org/documents/sluga.htm (on file with the *McGeorge Law Review*) ("T]he overwhelming majority hold that evidence of an ethics violation is admissible in a malpractice action.").

64. MODEL RULES PROF'L CONDUCT R. 1.6(a) (2012).

> impliedly authorized in order to carry out the representation or the disclosure is permitted by paragraph (b).[65]

Derived from agency law,[66] the duty of confidentiality is an integral part of the legal profession and is needed for effective client representation.[67] For example, without the duty of confidentiality criminal defense lawyers would be subject to constant government discovery threats and be unable to carry out the constitutionally guaranteed right to counsel.[68] While the duty of confidentiality is clear in theory, attorneys face difficulty in practice.

The duty of confidentiality has been modified over time to accommodate changing societal expectations for the roles of attorneys. Model Rule 1.6(b) provides some exceptions to confidentiality by authorizing a limited list of permissible disclosures.[69] For example, an attorney may disclose otherwise confidential information where the attorney reasonably believes disclosure will prevent death or substantial bodily harm;[70] prevent, mitigate, or rectify a client commission of fraud that damages financial or property interest of another;[71] or in order to comply with a court order.[72] In the early 2000s, the ABA added the exception for client fraud largely in response to the Enron scandal.[73] By amending the duty, the ABA showed that the obligations under confidentiality have shifted over time to address new issues.

Often considered alongside confidentiality, attorney-client privilege[74] and attorney work product[75] are important information protections in legal practice. Although similar in some respects, there are substantial differences in origin and scope between these concepts.[76] In the information age, attorneys have faced

65. *Id.*

66. RONALD D. ROTUNDA & JOHN S. DZIENKOWSKI, LEGAL ETHICS: THE LAWYER'S DESKBOOK ON PROFESSIONAL RESPONSIBILITY 227 (2011).

67. MODEL RULES PROF'L CONDUCT R. 1.6 cmt. 2 (2002) ("A fundamental principle in the client-lawyer relationship is that . . . the lawyer must not reveal information relating to the representation."). In reference to the protections of confidential communications between lawyer and client, Justice Rehnquist wrote:

> Its purpose is to encourage full and frank communication between attorneys and their clients and thereby promote broader public interests in the observance of law and administration of justice. The privilege recognizes that sound legal advice or advocacy serves public ends and that such advice or advocacy depends upon the lawyer's being fully informed by the client.

Upjohn Co. v. United States., 449 U.S. 383, 389 (1981).

68. U.S. CONST. amend. VI.

69. MODEL RULES PROF'L CONDUCT R. 1.6(b) (2011).

70. *Id.* R. 1.6(b)(1).

71. *Id.* R. 1.6(b)(2), (3).

72. *Id.* R. 1.6(b)(6).

73. ROTUNDA & DZIENKOWSKI, *supra* note 66, at 225 ("After the bankruptcy of the Enron Corporation and other scandals . . . the ABA House of Delegates adopted significant amendments to Rule 1.6 . . . .").

74. FED. R. EVID. 501 (2011).

75. FED. R. CIV. PROC. 26(b)(3) (2011).

76. *See* MODEL RULES PROF'L CONDUCT R. 1.6 cmt. 3 (2012) (explaining that confidentiality applies beyond evidentiary and discovery circumstances); ROTUNDA & DZIENKOWSKI, *supra* note 66, at 227

difficulties resolving issues for all three of these protections.[77] However, confidentiality stands out as unique as it is an ethical rule, as opposed to a law, and is a product of professional self-regulation.[78]

C. Model Rule 1.6(c)

In 2010, the ABA Commission on Ethics 20/20 sent an open letter to legal professionals and sought comments "to determine what guidance to offer to lawyers who want[ed] to ensure that their use of technology complies with their ethical obligations to protect clients' confidential information."[79] The Commission specifically identified the impact of cloud computing on confidential client information[80] and had the goal of "[offering] recommendations and proposals regarding how lawyers should address [the risks of inadvertent disclosure]."[81] As a result, the Commission eventually proposed paragraph (c) as an addition to Model Rule 1.6.[82] Model Rule 1.6(c) provides that:

> A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.[83]

Before adopting 1.6(c), the Model Rules merely provided reference to the potential issue of inadvertent or unauthorized disclosure in a comment to Model Rule 1.6.[84] The Commission based this rule in part on the previous iterations of Comments 16 and 17 from the 2002 edition of the Model Rules.[85] Comment 17 stated that a lawyer "must take reasonable precautions to prevent the information

(explaining that confidentiality is often considered wider but weaker than evidentiary privilege).

77. *See, e.g.*, John A. Wetenkamp, Note, *The Impact of E-Mail on Attorney Practice and Ethics*, 34 MCGEORGE L. REV. 135, 136–37 (2002) (discussing attorney use of email and confidentiality); *see generally* Adjoa Linzy, *The Attorney-Client Privilege and Discovery of Electronically-Stored Information*, 2011 DUKE L. & TECH. REV. 1 (2011) (discussing complications with privilege and e-discovery).

78. The Model Rules are a set of ethical rules written by attorneys to govern the conduct of attorneys as opposed to laws created by a legislature. *See generally* MODEL RULES OF PROF'L CONDUCT (2012) (serving as the model for most states ethics rules); Orin S. Kerr, *A Theory of Law*, 16 GREEN BAG 2D 111 (2012) (supporting the proposition).

79. Letter from ABA Comm'n on Ethics 20/20 Working Group on the Implications of New Technologies, to ABA Entities, Courts, Bar Associations, Law Schools, Individuals, and Entities (Sept. 20, 2010), at 1 [hereinafter Letter from Commission] (on file with the *McGeorge Law Review*).

80. *Id.*

81. *Id.* at 2.

82. COMMISSION RESOLUTION, *supra* note 8, at 4.

83. MODEL RULES PROF'L CONDUCT R. 1.6(c) (2012).

84. *Id.*1.6 cmt. 17 (2002) ("When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients.").

85. *Id.* R. 1.6 cmts. 16, 17.

from coming into the hands of unintended recipients."[86] Model Rule 1.6(a) uses the language "shall not,"[87] and Model Rule 1.6(b) uses the language "may."[88] Model Rule 1.6(c) differs by requiring the attorney to take affirmative steps to prevent a problem.[89] Because the rule requires taking action, rather than merely prohibiting particular action, it is essential for the attorney to understand what he or she must actually do.

The Commission provided a comment to Model Rule 1.6(c) ("Comment 18")[90] intended to offer guidance to attorneys.[91] The comment provides:

> Paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. . . . The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure.[92]

Under the comment's guidance, attorneys can consult a non-exhaustive list of factors to determine what constitutes "reasonable efforts" under Model Rule 1.6(c):[93]

> Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the

86. *Id.*

87. *Id.* R. 1.6(a) (2012).

88. *Id.* R. 1.6(b).

89. *Id.* R. 1.6(c) ("A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."); *see also* Letter from Charles E. McCallum, Chair, ABA Business Law Section Professional Responsibility Committee, to ABA Commission on Ethics 20/20 (Apr. 4, 2012) (on file with the *McGeorge Law Review*).

> Model Rule 1.6 (a) and (b) deal with restrictions on a lawyer's "revealing" information, i.e., a voluntary and knowing act by the lawyer. New subsection 1.6 (c) brings into the body of the Rule for the first time (although it is dealt with in Comments [16] and [17]) the requirement that the lawyer also "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information" relating to a client representation. *Id.*

90. The number of this comment changed during the drafting process. For ease of understanding, all references to the language will be referred to as Comment 18, which is consistent with Model Rule 1.6 as of 2012.

91. ABA COMM'N ON ETHICS 20/20, REPORT TO HOUSE OF DELEGATES 5 (2012), *available at* http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/20120508_ethics_20_20_final_resolution_and_report_technology_and_confidentiality_posting.authcheckdam.pdf [hereinafter Commission Report] (on file with the *McGeorge Law Review*).

92. MODEL RULE PROF'L CONDUCT R. 1.6 cmt. 18 (2012).

93. COMMISSION RESOLUTION, *supra* note 8, at 4–5.

> information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use).[94]

Comments to the Model Rules "do not add obligations," so Comment 18 functions only as "guidance for practicing in compliance" with Model Rule 1.6(c).[95] However, the comments in the Model Rules are particularly important because they address specific circumstances that are not covered by the general principles provided by the text of the rules.[96]

IV. ANALYSIS OF MODEL RULE 1.6(C)

This Part analyzes the origin and goals of Model Rule 1.6(c) and whether the rule will succeed as a practical guide when applied to attorney use of cloud computing. Next, this Part considers the intended beneficiaries of the rule. It concludes by proposing the ABA eliminate the factors in Comment 18 and replace them with a reference to standards of security as determined by experts in the field.

A. The Goals of the Rule

The Commission proposed Model Rule 1.6(c) after the legal community found a gap in the current ethics rules governing client confidentiality when using new technologies like cloud computing.[97] Many state and local bar associations attempted to fill this gap with formal opinions;[98] however, there remained an air of uncertainty, which prompted potentially over-the-top advice from some commentators.[99]

94. MODEL RULES PROF'L CONDUCT R. 1.6 cmt. 18 (2012).

95. *Id.* pmbl. & scope 14.

96. *See, e.g.*, *id.* R. 1.6 cmt. 6–12. (providing additional information on the disclosure exceptions that are potentially adverse to client interests). Some comment scenarios are also tested in the Multistate Professional Responsibility Exam, which all future attorney's must pass before admission to their respective bars. MPRE Subject Matter Outline (National Conference of Bar Examiners 2013) (on file with the *McGeorge Law Review*).

97. Letter from Commission, *supra* note 79, at 2 ("As an initial matter, the Commission recognizes that there may be a gap between technology-related security measures that are ethically required and security measures that are merely consistent with best practices.") (internal quotation marks omitted).

98. *See, e.g.*, State Bar of Nevada Standing Comm'n on Ethics and Prof'l Responsibility, Formal Opinion No. 33, at 1 (2006) ("If the lawyer acts competently and reasonably to ensure the confidentiality of the information, then he or she does not violate SCR 156 simply by contracting with a third party to store information . . . ."); Pennsylvania Bar Ass'n Comm'n on Legal Ethics & Prof'l Responsibility, Formal Opinion 2011-200 (2011); New York State Bar Ass'n Comm'n on Prof'l Ethics, Opinion 842 (2010).

99. *See* Brown, *supra* note 40, at 22 (suggesting that attorneys should know the geographic location of any data centers used to store their information for jurisdictional purposes).

Throughout the process of drafting its proposal, the Commission fielded a substantial amount of commentary from legal professionals and practice groups.[100] Many provided general support for the draft proposal text,[101] while others criticized and suggested changes.[102] Ultimately, the Commission recommended the ABA adopt Model Rule 1.6(c) and the accompanying comment[103] along with "the creation of a user-friendly, continuously updated website containing answers to common questions."[104]

The Commission had specific goals in mind when it made its proposal. First, the Commission intended to clarify the attorney obligation regarding inadvertent and unauthorized disclosure of confidential client information.[105] Attorneys have always had some duty to prevent disclosure of confidential client information,[106] but as attorneys have increased their use of computing technology, the waters have muddied regarding what must be done to protect confidentiality.[107] The rule was born out of a need for ethical guidance and clarity in the realm of new technology; the Commission specifically named attorney use of cloud computing as driving this need.[108] Since the Commission sought a rule to govern ethical—rather than merely "best practices"—use of cloud computing,[109] and since the ABA eventually adopted the proposal and incorporated the language into the Model Rules,[110] the ABA has seemingly endorsed the use of cloud computing for

100. *See Technology Comments Chart*, AM. BAR ASS'N (Apr. 17, 2012), http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/technology_working_group_comments_chart.authcheckdam.pdf (on file with the *McGeorge Law Review*).

101. Letter from Myles V. Lynk, Chair, ABA Standing Committee on Professional Discipline, to ABA Commission on Ethics 20/20 (Nov. 11, 2011); Letter from the Legal Cloud Computing Association, to Natalia Vera, ABA Center for Professional Responsibility (July 15, 2011) (on file with the *McGeorge Law Review*).

102. Comments on Revised Proposal on Technology and Confidentiality, Attorneys' Liability Assurance Soc'y, Inc. (Nov. 30, 2011) (on file with the *McGeorge Law Review*); Comments of Robert A. Creamer on Ethics 20/20, Robert A. Creamer (Nov. 29, 2011) (on file with the *McGeorge Law Review*).

103. COMMISSION RESOLUTION, *supra* note 8, at 4–5.

104. Letter from Jamie S. Gorelick and Michael Traynor, Co-Chairs, ABA Comm'n on Ethics 20/20, to ABA Entities, Courts, Bar Associations, Law Schools, and Individuals (Dec. 28, 2011), *available at* http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/20111228_summary_of_ethics_20_20_commission_actions_december_2011_final.authcheckdam.pdf (on file with the *McGeorge Law Review*).

105. COMMISSION REPORT, *supra* note 91, at 4.

106. *Id.* ("Although this obligation is described in Comments [16 and 17 of the 2002 edition of the Model Rules], the Commission concluded that technology has made this duty sufficiently important that it should be elevated to black letter status in the form of the proposed Model Rule 1.6(c).").

107. *See* Stephens, *supra* note 37, at 241–43 (discussing the inadequacy of the previous test for "reasonable precautions" under the Model Rule comments); *supra* note 98 (providing various tests as determined by state bar associations). Although the lack of clarity as to professional ethics obligations was noted by many, it was up to the ABA, who composes the Model Rules, to provide guidance since the earlier rule proved unworkable and lacked clout.

108. Letter from Jamie S. Gorelick and Michael Traynor, *supra* note 103 ("Client confidences are no longer kept just in file cabinets, but on laptops, smart phones, tablets, and in the cloud.").

109. Letter from Commission, *supra* note 79, at 2.

110. *See Ethics 20/20 Rule Changes Approved by ABA Delegates with Little Opposition*, BLOOMBERG (Aug. 15, 2012), http://www.bna.com/ethics-2020-rule-n12884911245/ (announcing the approved changes,

the practice of law. This endorsement supports the notion that the ethical clarification was needed.

Second, the Commission intended to provide guidance for attorney use of new technology in light of the associated confidentiality risks.[111] Related to this, the Commission also had the implicit goal of keeping the language of the rule relevant and applicable. Attorneys need to understand how to practice within ethical rules if those rules are to have any positive effect on them. Since the Commission acknowledged that technology would likely outdate any specific language in the rule[112] and intended a new rule to "reflect the realities of 21st century law practice,"[113] the Commission necessarily intended Model Rule 1.6(c) to remain relevant as technology progresses and use becomes more prevalent.

The Commission must have also intended attorneys to apply the rule in their daily practices. The Commission proposed an interpretive resource in the form of an amendment to the official comments to aid in application.[114] Additionally, the official comment provides that "[a] client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule."[115] The rule must be applicable to practice if it has the potential to create waivable security measures.[116]

B. Analysis of the Rule

The Commission had several goals when proposing Model Rule 1.6(c).[117] From the perspective of an attorney using cloud computing, the rule may not adequately meet all of these goals because it sacrifices applicability for relevancy. However, it only takes a slight rewriting of the official comment to overcome this problem.[118]

1. The Benefits and Challenges of Vagueness

When reading Model Rule 1.6(c) to discover what it adds to or clarifies regarding attorney's ethical obligations, one quickly realizes that the text is vague.[119] In the context of an ethical rule, vagueness creates benefits and

including Model Rule 1.6(c)).

111. COMMISSION REPORT, *supra* note 91, at 2.

112. *Id.* at 5.

113. *Id.* at 3.

114. MODEL RULES PROF'L CONDUCT R. 1.6 cmt. 18 (2012).

115. *Id.*

116. *Id.*

117. *Supra* Part IV.A.

118. *See infra* Part IV.C (proposing an amendment to the interpretive comment).

119. *See* MODEL RULES PROF'L CONDUCT R. 1.6(c) (2012).

challenges. By using vague language, Model Rule 1.6(c) avoids the pitfall of becoming antiquated.[120] Since technology use prompted the rule,[121] the Commission wisely avoided using specific language that would quickly become outdated due to the relatively fast moving world of computing technology.[122] Cloud computing, which prompted the rule because of the difficulty in applying existing black-letter ethical obligations, will not necessarily operate or exist in its contemporary form as the technology continues to change.[123] Further, since the ABA updates the Model Rules infrequently,[124] language related to specific technology operations would become outdated faster than the ABA would promulgate and implement new rules.[125]

On the other hand, by using vague "reasonableness" language, attorneys have little guidance in applying Model Rule 1.6(c) to their practice. The standard of reasonableness is used generally throughout the law but has little meaning without interpretive guidance.[126] The Commission recognized this issue and recommended adopting Comment 18 to assist attorneys in interpreting their obligation of taking "reasonable efforts."[127] The Commission also "recommended that the ABA create a centralized website that contains continuously updated and detailed information about data security."[128] Attorneys may find the guide useful, but it would not aid in interpreting Model Rule 1.6(c) so much as it would provide a resource for becoming informed about data security because it is not officially part of the Model Rules.[129]

120. *Id.*

121. COMMISSION ISSUES PAPER, *supra* note 3, at 1.

122. MODEL RULES PROF'L CONDUCT R. 1.6(c); *see generally Moore's Law Inspires Intel Innovation*, INTEL CORP., http://www.intel.com/technology/mooreslaw (last visited Jan. 7, 2014) (on file with the *McGeorge Law Review*) ("Moore's Law. . . states that the number of transistors on a chip will double approximately every two years."). Moore's Law is generally credited as the most accurate prediction as to the perpetually accelerating development of new technology. *E.g.*, John O. McGinnis, *Laws for Learning in an Age of Acceleration*, 53 WM. & MARY L. REV 305, 312 (2011) ("This prediction, which has been approximately accurate for the last forty years, means that almost every aspect of the digital world—from computational calculation power to computer memory—is growing in density at a similarly exponential rate.") (internal citations omitted).

123. *See supra* Part IV.A.

124. The ABA last adopted a major update the Model Rules in 2003 after the Enron scandal. MODEL RULES PROF'L CONDUCT Preface (2013).

125. COMMISSION REPORT, *supra* note 91, at 5.

126. *E.g.*, RESTATEMENT (SECOND) OF TORTS § 283 (1965) ("[T]he standard of conduct to which he must conform to avoid being negligence is that of a reasonable man under like circumstances."). Although Model Rule 1.0(h) defines reasonable as "denot[ing] the conduct of a reasonably prudent and competent lawyer," this only directs against whom "reasonable" is determined rather than how. MODEL RULES PROF'L CONDUCT R. 1.0(h) (2012). Further, there are issues with assuming the phrase "reasonable efforts" necessarily uses the definition of the word "reasonable" in Model Rule 1.0(h). *See infra* Part IV.B.3.

127. Commission Report, *supra* note 91, at 4–5.

128. *Id.* at 5.

129. *Id.*

2. Issues with Interpreting "Reasonable Efforts"

The Commission acknowledged the rapid pace of technology changes but still chose to provide specific factors under Comment 18 "that lawyers should consider when determining whether their efforts are reasonable."[130] In an attempt to provide guidance, the Commission took a different approach to the comment factors than they did to the rule itself by using specific language.[131]

As discussed previously, using specific language in the technology context hurts, rather than helps, application of law because technology advances at such a swift pace.[132] This is especially true when the language is enshrined in the Model Rules because amendments to the rules are so rare.[133] By the time new rules are adopted, specific technologies may function differently or be near extinction.[134]

Regarding individual factors, Comment 18 has many interpretive struggles. For example, the "likelihood of disclosure" factor refers to the probability of disclosing client information by accident or as a result of hacking.[135] On the one hand, both of these possibilities are inherently unpredictable and therefore elude accurate determinations of likelihood by an attorney. Obviously, if one could predict hacking, then one could take sufficient steps to prevent and thereby eliminate the problem, which would render the factor irrelevant to the determination of reasonable efforts.[136] This is also true of accidents and human error.[137] On the other hand, attorneys do not need mathematic or scientific accuracy in determining the content or weight of a factor. Developed by Judge

130. *Id.*

131. *See supra* Part III.C (listing the various factors).

132. *See supra* note 122.

133. The ABA last adopted a major update to the Model Rules in 2002.

134. *See, e.g.*, Dan Tynan, *10 Technologies That Should Be Extinct (But Aren't)*, PC WORLD (Jul. 4, 2010, 6:40 PM), http://www.pcworld.com/article/200325/10_technologies_that_should_be_extinct.html (on file with the *McGeorge Law Review*) ("These screechy, annoying gadgets [fax machines] continue to attract realtors, lawyers, insurance companies, and others nervous about the authenticity of signed documents without an ink-based John or Jane Hancock on them.").

135. MODEL RULES PROF'L CONDUCT R. 1.6 cmt. 18 (2012).

136. The FBI provides information regarding online scams and virus warnings as well as its recommendations for prevention; however, outside of general safety tips, specific information regarding instances of hacking only comes after the fact. *New E-Scams & Warnings*, FBI, http://www.fbi.gov/scams-safety/e-scams (last visited Feb. 24, 2014) (on file with the *McGeorge Law Review*); *see also* Letter from Charles E. McCallum, Chair, ABA Business Law Section Professional Responsibility Committee, to ABA Commission on Ethics 20/20 (Apr. 4, 2012) (on file with the *McGeorge Law Review*) ("As to hacking, it appears that even very large and well funded governmental entities and large corporations, in each case with large and expert staffs, access to highly capable consultants, and ability to invest in expensive and sophisticated data security systems, are vulnerable to hacking.").

137. While it may be theoretically true that human error could be predicted, these theories are still in early stages of development. *See generally Early Warning System*, THE ECONOMIST (Apr. 26, 2008), http://www.economist.com/node/11088585 (on file with the *McGeorge Law Review*) (discussing the work of researchers attempting to predict human error in repetitive tasks).

Learned Hand in *United States v. Carroll Towing Co.*,[138] the Hand formula in negligence analysis requires weighing several factors and does not require specific quantities.[139] Instead, it is sufficient for purposes of the formula to find that a factor is "higher" or "lower," "greater" or "lesser."[140] Because one can legitimately determine factors with relative language, as shown by Judge Hand's analysis,[141] the factors in Comment 18 would be sufficient if an attorney can reasonably determine their general content.

Those attorneys who lack much technological understanding will, however, find determining the general content of the factors in the comment difficult due to a lack of familiarity. This deficiency in knowledge would inhibit intuitive determinations that are easier to form in other areas. For example, an attorney may intuitively determine that a copy shop staffed by an inattentive teenager is less secure than a bank vault. This same intuitive sense is more difficult for attorneys using cloud computing because the attorney-user may lack sufficient knowledge to make this type of determination.[142] For many people, the ability to say that one form of encryption employed by a cloud computing provider is comparatively better than another is not as easy as judging the storm-born danger of a tethered vessel, as seen in *Carroll Towing*.[143]

Even if there existed a general understanding sufficient to intuitively say extra safeguards are needed to prevent disclosure, applying the Comment 18 factors requires assuming that safeguards exist and that they are deployable. Cloud computing providers may not be willing to accommodate a single user with requests for additional security as it would require admitting that their typical security could be inadequate for customer safety.[144] Although the client is free to request special levels of heightened or relaxed precautions,[145] this does not answer what default level of precautions are needed to satisfy the ethically imposed "reasonable efforts" without obtaining a client waiver.[146]

138. 159 F.2d 169 (1947).

139. *Id.* at 173 ("[T]he owner's duty, as in other similar situations, to provide against resulting injuries is a function of three variables: (1) The probability that she will break away; (2) the gravity of the resulting injury, if she does; (3) the burden of adequate precautions. Possibly it serves to bring this notion into relief to state it in algebraic terms: if the probability be called P; the injury, L; and the burden, B; liability depends upon whether B is less than L multiplied by P: i.e., whether B < PL.").

140. *Id.* ("[T]he likelihood that a barge will break from her fasts and the damage she will do, vary with the place and time; for example, if a storm threatens, the danger is greater . . . .").

141. *Id.*

142. *See infra* Part IV.C (discussing the intended audience).

143. 159 F.2d at 173.

144. Dropbox declares that "[y]our stuff is safe." *Features*, DROPBOX, http://www.dropbox.com/features (last visited Jan. 7, 2014) (on file with the *McGeorge Law Review*).

145. MODEL RULE PROF'L CONDUCT R. 1.6(c) cmt. 18 (2012).

146. *Id.* Clients can waive the use of additional safeguards, but this assumes that safeguards exist and that they are capable of being used because, otherwise, there is nothing for the client to waive. *Id.*

3. Practical Challenges in Application

Beyond interpretation issues, attorneys will face difficulty with the procedural aspects of applying the test for "reasonable efforts."[147] Compounded with the issues in determining the substantive meaning of the factors, the provided test for determining reasonable efforts under Model Rule 1.6(c) remains unwieldy.

Factor tests are nothing new. Tort law has the *Rowland* factors,[148] civil procedure has the *Asahi* factors,[149] and corporate law has the piercing factors.[150] Rarely will a test have precise rules of application at its inception because these doctrines are generally developed over time.[151] As common as factor tests are in the law, there can be extensive issues in application where there is little guidance.[152] Here, where attorneys need a clear rule to apply to their practices, the lack of guidance for using factors adds to their pre-existing shortcomings.[153]

One way to clarify what practices constitute reasonable efforts under Model Rule 1.6(c) is judicial or administrative interpretation. Rulings would offer clarity on both the proper substantive interpretation of the individual factors as well as how to apply them procedurally. There are, however, two problems with this wait-and-see approach. First, an interpretation of "reasonable efforts" regarding one technology may become outdated by the time it is actually applied due to the speed at which technology develops. Second, Model Rule 1.6(c) and Comment 18 are unlikely to receive enough interpretation to develop a proscriptive scheme because the Model Rules are not actual law.[154]

It takes time for vague language to develop sound meaning. Justice Cardozo, for example, famously confused all with his statement that members of a

147. *Id.*

148. Rowland v. Christian, 69 Cal. 2d 108, 117 (1968).

149. Asahi Metal Indus. Co. v. Superior Court, 480 U.S. 102, 113 (1987).

150. *See, e.g.*, DeWitt Truck Brokers v. W. Ray Flemming Fruit Co., 540 F.2d 681, 686–87 (1976) (providing a list of factors to use in piercing the corporate veil); FRANKLIN A. GEVURTZ, CORPORATION LAW § 1.5 (2d ed. 2010) (explaining and criticizing the various factors used to determine whether to pierce the corporate veil).

151. *Compare* Carroll Towing Co., 159 F.2d at 173 (announcing a precise formula for assessing negligence), *with* GEVURTZ, *supra* note 150, at § 1.5 (asserting that, "despite hundreds of opportunities to get it right, judicial opinions in [the area of piercing the corporate veil] have made it one of the most befuddled.").

152. Judge Posner in *Exacto Spring Corp. v. Comm'r* mirrors these applicatory concerns when reviewing a similarly vague multifactor test put forward by a lower court. 196 F.3d 833, 835 (1999) (criticizing, at length, the use of a "nondirective" test where "[n]o indication is given of how the factors are to be weighed . . . ."). The court criticizes the test for using factors that "do not bear a clear relation to either each other or to the primary purpose" of the statute at issue and that "because of its nondirective character, [the test] invites the making of arbitrary decisions based on uncanalized discretion . . . ." *Id.*

153. One is reminded of Justice Scalia's famous response to the factor test in *Bendix Autolite Corp. v. Midwesco Enters., Inc.*, where he disapprovingly declares, "[The Pike balancing test] is more like judging whether a particular line is longer than a particular rock is heavy." 486 U.S. 888, 897 (1988) (Scalia, J., dissenting).

154. *See* Part III.A (discussing the Model Rules).

partnership owe each other "[n]ot honesty alone, but the punctilio of an honor . . . ."[155] This statement has been subject to years of scrutiny and only now contains an allegedly applicable meaning.[156] Comments to the Model Rules are unlikely to receive such scrutiny because they "do not add obligations . . . [and exist only to] provide guidance for practicing in compliance with the Rules."[157] Additionally, even though the language of Model Rule 1.6(c) will likely be adapted to state ethical codes, technology may outpace any eventual interpretation given to these words.[158] Waiting for a court to interpret a rule does not solve the problem of present-day attorneys who wish to improve their practice with cloud computing but are fearful of the seemingly looming ethics issues.[159]

Ultimately, the comment factors do not provide an adequate framework for determining whether an attorney has made reasonable efforts to prevent access to or disclosure of confidential information. Thus, an attorney following the factors in Comment 18 will be forced to rely on intuition alone. As a result, the attorney might unintentionally act discordantly with respect to the duty of confidentiality under Model Rule 1.6(c). This outcome would be completely at odds with the Commission's goals for the rule.[160]

4. The Intended Recipients of the Rule

The intended beneficiaries are important to identify for purposes of Model Rule 1.6(c) because it sheds light on how the rule should be interpreted. Model Rule 1.0 explains much of the legal terminology used throughout the rules, and although it includes definitions of "reasonable,"[161] "reasonable belief,"[162] and "reasonably should know,"[163] it does not define the phrase "reasonable efforts."

155. Meinhard v. Salmon, 249 N.Y. 458, 464 (1928).

156. Marleen A. O'Connor, *How Should We Talk About Fiduciary Duty? Directors' Conflict-of-Interest Transactions and the ALI's Principles of Corporate Governance*, 61 GEO. WASH. L. REV. 954, 966 (1993) ("This forceful rhetoric suggests a moral mandate that no fiduciary may attempt to secure any private advantage at the expense of the beneficiary. Although some commentators may dismiss the language as mere ornamentation, this position fails to account for the way that the *Meinhard* dictum has endured the test of time.").

157. MODEL RULES PROF'L CONDUCT pmbl. 14 (2012).

158. *Supra* Part IV.B.1.

159. *Supra* Part II.C.

160. *Supra* Part IV.A.

161. *Id.* R. 1.0(h) ("'Reasonable' or 'reasonably' when used in relation to conduct by a lawyer denotes the conduct of a reasonably prudent and competent lawyer.").

162. MODEL RULES PROF'L CONDUCT R. 1.0(j) (2012) ("'Reasonable belief' or 'reasonably believes' when used in reference to a lawyer denotes that the lawyer believes the matter in question and that the circumstances are such that the belief is reasonable.").

163. *Id.* R. 1.0(i) ("'Reasonably should know' when used in reference to a lawyer denotes that a lawyer of reasonable prudence and competence would ascertain the matter in question.").

If "reasonable efforts" ought to be construed consistently with the use of "reasonable," as a defined term in the Model Rules, then interpreting Model Rule 1.6(c) would require considering the practices of other "reasonably prudent and competent lawyer[s]."[164] Alternatively, since the Commission necessarily intended the rule to be applicable,[165] it is important to understand who the Commission intended the rule for when determining whether it meets its goals. Either way, because attorneys fall on a wide spectrum of technology competency, and because Model Rule 1.6(c) is difficult to apply, some clarity regarding a possible solution to the problem may emerge when the intended beneficiaries of the rule are identified.

With regard to attorneys that use technology, there are four basic groups.[166] First, there are those attorneys who adopt new technologies quickly. For these attorneys, a higher level of technology competency can be assumed due to familiarity and an interest in the area. These attorneys are on the cutting edge of technologies and share their discoveries with others. Second, there are those attorneys that adopt new technologies but may not quite understand them. This might effectively be demonstrated by many of the younger attorneys that are facially familiar with numerous aspects of technology. Although comfortable as an end-user, these attorneys lack much depth as to how the particular technology works or what potential issues may arise. Third, there are those attorneys that use technology in their practices but have either no time or no interest in gaining a deeper understanding. Last, there are those attorneys that refuse to accept new technology in their practices.

Though not with intention, this last group of attorneys will increasingly encounter new technology as it becomes more integrated in the practice of law. For example, some courts, including the federal judiciary, use websites for e-filing and posting of tentative rulings.[167] If an attorney actively rejects technology, then he is unable to use these services and has increased trouble litigating, especially against those attorneys who wholly embrace it.[168] Further, attorneys

164. *Id.* R. 1.0(h).

165. *Supra* Part IV.A–B.

166. The reality is that familiarity and interest with technology falls on a spectrum, and these categories are therefore acknowledged to be arbitrary yet still useful for explanatory purposes.

167. *See, e.g.*, *Online Services*, THE SUPERIOR COURT OF CAL. CNTY. OF S.F., http://www.sfsuperior court.org/online-services (last visited Jan. 7, 2014) (on file with the *McGeorge Law Review*) (providing access to court services for civil cases filed in San Francisco County); PACER, http://www.pacer.gov/ (last visited Feb. 2, 2014) (on file with the *McGeorge Law Review*) ("Public Access to Court Electronic Records (PACER) is an electronic public access service that allows users to obtain case and docket information from federal appellate, district and bankruptcy courts . . . .").

168. For instance, it would be difficult to effectively communicate with those attorneys that operate "virtual private law offices" and almost exclusively do their business online. *See supra* note 18. It is, of course, unlikely that an attorney would reject the Internet entirely because he or she would instead use a staff member as a liason. *E.g.*, Thomas, *supra* note 36 (supposing that "[p]erhaps [the] old guy who never got a computer and gets his secretary to print all his emails for him to read has it right after all" after the attorney experienced cloud service downtime).

may find it hard to avoid cloud computing if it continues to be incorporated into the profession similarly to now-standard tools like Internet-based legal research.[169]

Although ethics rules govern all attorneys, the intended beneficiaries are relevant in determining applicability because it can help identify how the Commission intended the goals be achieved.[170] If the rule was intended for attorneys on the end of the spectrum closer to the first category—attorneys who adopt new technologies quickly—then the factors would make more sense, excusing the other problems, because there is a generally stronger familiarity with technology. However, it is more likely that attorneys in categories two or three would need a rule guiding their use because they may not understand the ramifications of certain actions on confidentiality. If this is the case, then the factors do not assist, and the test remains unworkable.

By explicitly acknowledging the categories of users, a proposal to aid in interpreting the language of Model Rule 1.6(c) can be specifically tailored to account for those who will likely find trouble in its application. It is likely that the attorneys in the first category will know to take necessary precautions because they would be more familiar with the threats and risks of error. It also seems that the intended beneficiaries of the rule include attorneys who want to use or are required to use a particular new technology but do not have a thorough understanding of how it works.[171] Because these attorneys need not gain an insider-level of knowledge about a service they choose to use, nor would they have the time, interest, or patience to do so, it is important to ensure the rule accounts for this reality while promoting the duty of confidentiality.

C. Proposal

The ABA should amend Comment 18 to adequately meet all of the Commission's goals for Model Rule 1.6(c).[172] The rule will likely remain relevant due to its vague "reasonableness" language,[173] but attorneys will have trouble applying it to their daily practices. Because this is an ethical rule designed for attorneys to apply to their practices in order to clarify and avoid confidentiality

169. *See, e.g.*, Laura K. Justiss, *A Survey of Electronic Research Alternatives to LexisNexis and Westlaw in Law Firms*, 103 LAW LIBR. J. 71 (2011) (discussing a number of digital databases and docket services that are used in practice as an alternative to the ever-pervasive Westlaw and Lexis).

170. *See supra* Part IV.A (discussing these goals).

171. For instance, an attorney at a law firm, business, or governmental agency may be forced to use a service in his or her practice as a policy for the organization even if the attorney is not interested. Alternatively, younger attorneys may have been raised with their fingers on keyboards and thus fail to look both ways before crossing the proverbial technology street by forgoing an adequate understanding as to the technologies they use.

172. *Supra* Part IV.A.

173. *Supra* Part IV.B.1.

breaches, especially when using new technologies like cloud computing, attorneys must be able to actually apply the rule.

1. Determine Reasonable Efforts by Looking to Experts

The ABA should amend the language of Comment 18 to change the burden of determining what technology is safe for use from *on the attorney* to *on experts in the particular field*. In place of the factor test language, Comment 18 could instead read:

> The standard of reasonable efforts required by the rule is met if the level of safety and preparation taken to avoid inadvertent or unauthorized disclosure is consistent with what a reputable expert in the relevant field finds is necessary to sufficiently safeguard confidential information.

This change allows Model Rule 1.6(c) to accomplish all of the Commission's goals.[174] First, by looking to reputable experts in the relevant field, the means of interpreting Model Rule 1.6(c) would remain relevant as technology changes. Expert knowledge is more likely to be up-to-date on the current trends, and the test would not fall subject to the issues associated with specific language becoming outdated.

Second, replacing the factor test in Comment 18 with the proposed language would provide a standard that attorneys can actually apply. Looking to experts in the field to determine the safety of particular technologies would avoid the problem of varied sophistication levels.[175] Since there would be no factors to weigh, attorneys of all skill levels could apply the test. Additionally, since there would be no factor test, the procedural shortcomings would not need to be solved.[176] For example, an attorney interested in adopting a cloud computing service could consult with or research the opinions of qualified computer professionals about the security of that encryption type or the reputation of that provider. If the service in question is considered secure enough for the needs of the attorney by those most familiar with it, then the attorney would be acting accordantly with Model Rule 1.6(c) by taking efforts consistent with this better understanding of protecting the confidential information.

One anticipated criticism of this proposal is the difficulty of determining what level of knowledge qualifies as reputable. However, reputability could be determined through the standards of the particular field. Evidence law has grappled with a similar struggle in the admission of scientific evidence through the *Daubert*[177] and *Frye*[178] standards. Unlike the more rigid *Frye* standard, which

174. *See supra* Part IV.A (discussing these goals).

175. *See supra* Part IV.B.4 (discussing the four possible technology sophistication levels of attorneys).

176. *See supra* Part IV.B.3 (explaining the procedural challenges).

177. Daubert v. Merrell Dow Pharmaceuticals, 509 U.S. 579, 597–98 (1993).

requires a "general acceptance" of a scientific theory offered before it is admissible in court,[179] attorneys using the proposal would invoke a more *Daubert*-like standard, in that reputability stands more as a gatekeeper. Then, whether a particular technology would be on par with what is needed to safeguard confidential client information could be understood by comparing it to what a reputable expert finds or would find secure, rather than requiring the exact technology actually be accepted by the field.

For example, if an attorney adopted a new, experimental form of data storage, an expert might advise additional data back-up to conventional forms of storage due to a prevalent attitude that the form of storage in question is less stable. If an attorney in this hypothetical followed the expert's advice regarding the prevalent attitudes, then the attorney would have met the ethical duty to take reasonable steps to avoid the unauthorized or inadvertent disclosure of confidential client information, assuming he or she continues to act accordingly. But if the expert advised the attorney that the host of a technology had a history of using inadequate measures in areas such as encryption, building security, power source stability, or data storage redundancy, then the attorney should likely seek an alternative service.

Of course, the attorney need not necessarily speak to an expert to determine whether a particular technology meets the standard. If the attorney is capable, he or she could conduct an independent inquiry into expert literature to determine what a reputable expert would find as adequate. This proposal does not necessitate consulting an expert but rather uses the information gleaned from an expert opinion as a basis for determining adequate security and thus reasonable efforts.

2. Feasibility and Benefits of the Proposal

This proposed test would work in conjunction with the Commission's proposed data security guide.[180] This guide would serve as a vehicle for sharing information regarding particular services as well as providing information on data security as the Commission intended.[181] Since the Commission wrote Model Rule 1.6(c) to clarify the ethical duty and not merely "best practices," the guide currently fails to support the rule. Under this proposal, the guide could serve as a central information dispenser regarding meeting the duty as opposed to its current enigmatic general role. By not limiting the source of information used to

178. Frye v. United States, 293 F. 1013, 1014 (D.C. Cir. 1923).

179. *Id.* ("[W]hile courts will go a long way in admitting expert testimony deduced from a well-recognized scientific principle or discovery, the thing from which the deduction is made must be sufficiently established to have gained general acceptance in the particular field in which it belongs.").

180. COMMISSION REPORT, *supra* note 91, at 5.

181. *Id.* ("[T]he Commission has recommended that the ABA create a centralized website that contains continuously updated and detailed information about data security.").

determine whether reasonable efforts have been taken, but instead using the guide as a possible tool for gathering the information requested by the proposed amendment, the ABA would show its dedication to reaching all of the goals of Model Rule 1.6(c).[182]

Further, moving specific language regarding security out of Comment 18 reduces the chance that the rule will become outdated and require subsequent amendment when new technologies develop that may not comport to the current language. This is because the guide can be readily updated to remain consistent with expert opinion.

By positioning the burden of determining whether a particular service is adequately secure on the shoulders of experts familiar with the technology, the concern regarding varying sophistication level of attorneys is removed.[183] Eliminating the troublesome factor analysis means more attorneys can adopt time- and money-saving technologies and find comfort knowing that consulting and acting in accordance with experts is sufficient to satisfy this portion of confidentiality. Essentially, the attorney would simply conduct a type of due diligence on a service to satisfy the requirements of Model Rule 1.6(c).

This is not the first time in which a Model Rule has looked outside of the text for interpretative guidance.[184] The previous iteration of Comment 17 in the 2002 edition of Model Rule 1.6 did not require an attorney to "use special security measures if the method of communication affords a reasonable expectation of privacy" when taking reasonable precautions to prevent disclosure.[185] While this demonstrates that it is not novel to propose an external means of interpretation, problems arose in practice with this example because the language references another body of law—the reasonable expectation of privacy—in an area that had yet to be fully developed for Internet technologies.[186] This proposal avoids this issue by referencing a source of information outside of the slower-moving legal world as opposed to one reliant on it; the means of determining reasonable efforts are instead kept consistent with the continually advancing technology it is designed to address through flexible and adaptive language.

This proposal is feasible because it is a mere amendment to an existing comment in the Model Rules. Although the rule and the comment have already been officially approved and incorporated into the Model Rules,[187] amending a

182. *Supra* Part IV.A.

183. *Supra* Part IV.B.4.

184. MODEL RULE PROF'L CONDUCT R. 1.6 cmt. 17 (2002).

185. *Id.*

186. *See* Stephens, *supra* note 37, at 242–43 ("The answer of whether a reasonable expectation of privacy exists in a method of communication is not simple. . . . The Supreme Court has not yet addressed the issue of whether a reasonable expectation of privacy exists in the contents of email.").

187. *See Ethics 20/20 Rule Changes Approved by ABA Delegates with Little Opposition*, BLOOMBERG BNA (Aug. 15, 2012), http://www.bna.com/ethics-2020-rule-n12884911245/ (on file with the *McGeorge Law Review*) (announcing the approved changes, including Model Rule 1.6(c)).

comment to the Model Rules would be simpler than proposing an entirely new rule, which could take years. Further, since it is a relatively minor textual alteration that would result in a substantial benefit, the opportunity cost is low. Thus, there is a strong incentive to adopt this change.

V. CONCLUSION

Attorneys benefit considerably from integrating cloud computing services into their practices. Benefits of cloud computing services include decreased cost and increased efficiency, but there are real risks posed because of malicious attacks and human error.[188] Attorneys who want to benefit from incorporating cloud computing into their practices should do so consistent with their ethical obligations to avoid risks to their client's confidentiality.

Model Rule 1.6(c) signals that the profession is interested in promoting the use of new technologies like cloud computing. The rule partially exists as evidence that the ABA is comfortable with an increasingly technology-reliant practice of law.[189] The rule itself succeeds in its goal of remaining relevant because the reasonableness language in Model Rule 1.6(c) will not need revision when the next practice-changing technology arrives.[190] On the other hand, one of the most important goals of Model Rule 1.6(c)—providing attorneys will a rule to ethically guide their conduct—is not achieved in the current iteration.[191] With a minor change in the interpretive comment to focus on expert guidance in determining reasonable efforts, however, the rule would meet all of the ABA's intended goals, giving attorneys a clear and applicable ethical standard that will remain relevant over time.[192]

188. *See supra* Part II.B–D (explaining and evaluating the risks and benefits).

189. *See supra* Part IV.A (identifying the goals for the rule, which includes an interest in ethically governing use, rather than prohibiting it).

190. *See supra* Part IV.B.1 (arguing one benefit of vague "reasonableness" language is prolonged relevance through future adaptability).

191. *See supra* Part IV.B.2–4 (arguing the issues involved with current means for determining "reasonable efforts" under the rule).

192. *See supra* Part IV.C .1 (proposing an amendment to the comment interpreting the rule).