Campbell Law Review

Volume 36
Issue 1 *Fall 2013*

Article 6

2014

Dropping Dropbox in your Law Practice to Maintain your Duty of Confidentiality

Eliu Mendez

Dropping Dropbox in your Law Practice to Maintain your Duty of Confidentiality

INTRODUCTION[1]

A search for the term "cloud" on Google no longer returns the familiar images of cumulus, stratus, and nimbus clouds. Rather, the search returns a flurry of cloud computing sources, advertisements and articles. Over the past few years, the general public has become increasingly familiar with the concept of cloud computing.[2] Indeed, the general public has been using cloud functionality since the early days of America Online Mail.[3] Modern technology, an evolving concept by infinite architects, is hard to define, and cloud computing is no different.[4]

In very basic terms, cloud computing is a service that allows users to locally access an external server via a network or an Internet connection, thus permitting users to store and retrieve information and data in places other than on their own "home" network.[5] In more technical terms, cloud computing is the outsourcing of third-party services,[6] which may be accessed remotely over a network, usually the

1. I want to thank my wife, Bethany, for her patience and support not only during the writing of this Comment, but also throughout law school. I would also like to thank Professor Bobbi Jo Boyd for offering feedback and direction when my Comment needed it most. Lastly, I want to thank you for taking the time to read my Comment.

2. Examples of everyday uses of cloud computing services include online data storage (*e.g.*, Dropbox or iCloud), Internet based e-mail (*e.g.*, Gmail), or software as a service (SaaS) (*e.g.*, Amazon Web Services or Microsoft Office 365).

3. *See* AOL, http://www.aol.com/ (last visited Nov. 2, 2013) (noting the familiar, original welcome screen, "You've Got Mail!").

4. Eric Knorr & Galen Gruman, *What Cloud Computing Really Means*, INFOWORLD (Apr. 7, 2008), http://www.infoworld.com/d/cloud-computing/what-cloud-computing-really-means-031 (defining cloud computing narrowly as "virtual servers available over the Internet," or broadly as any service used "outside the firewall").

5. *See* Natalie R. Kelly, *Kickin' Around in the Cloud: Lawyers and Cloud Computing 101*, 16 GA. B.J., June 2011, at 62, 62. Cloud computing is basically "a system[] where some component of the technology is either accessed or resides on an external server or servers; or the computing process happens wholly or in part and is accessed over the Internet." *Id.*

6. These are most commonly software, platforms, or infrastructure services.

Internet.[7]

One of the most prevalent cloud computing services is Dropbox.[8] Dropbox is a free file-hosting service that offers cloud storage and file synchronization.[9] Dropbox is quickly becoming the staple of cloud computing storage because it is easy to use, free, and allows you to "be anywhere."[10] The legal profession does not escape Dropbox's appeal,[11] and it is important that attorneys using Dropbox recognize the risks involved, including the possibility of putting their licenses in jeopardy.

This Comment explores cloud computing within the practice of law. This Comment first discusses the advantages and disadvantages of cloud computing, specifically those that may affect the practice of law. Second, this Comment examines the developing legal and ethical issues that arise from the use of cloud computing technology, primarily Dropbox. After a brief introduction to the American Bar Association (ABA) and the North Carolina State Bar, this Comment analyzes three amendments to the Model Rules of Professional Conduct that were introduced by the ABA Commission on Ethics 20/20. It then addresses the consequences that these amendments have on preserving the attorney's duty of confidentiality when using cloud computing technology. Finally, after illuminating the gaps in the current unamended rules, this Comment introduces recommendations to better protect both attorneys and the public from unauthorized disclosure of confidential client information as a result of an inadvertent breach of the duty of confidentiality.

---

7. Gavin Hume, *Use of Cloud Computing by Lawyers Requires Due Diligence to Stay Onside Regulatory Requirements*, 70 ADVOC. VANCOUVER 51, 51 (2012) ("Examples of cloud computing services that are commonly used include webmail, such as Gmail, and services such as Dropbox, Facebook and LinkedIn. In some instances, services are free (often supported by advertising); in other cases, they are charged on a pay per usage basis."). *See* Larry Port, *Resources in the Clouds*, 28 GPSOLO, Dec. 2011, at 28, 29 ("[S]imple definition: The cloud allows users to consume computing resources that they don't have locally in their office . . . without having to install it, upgrade it, or purchase or maintain hardware for it.").

8. *About Dropbox*, DROPBOX, https://www.dropbox.com/about (last visited Nov. 3, 2013) (claiming that "more than 200 million people across every continent use Dropbox").

9. *Id.*

10. *Be Anywhere*, DROPBOX, https://www.dropbox.com/tour/2 (last visited Nov. 3, 2013).

11. *See* Stephan Futeral, *Ipad Apps for Practicing Law in the "Post-PC" Era*, S.C. LAW., May 2013, at 35, 40.

I. THE ADVANTAGES AND DISADVANTAGES OF CLOUD COMPUTING SERVICES

A. The Practical Benefits of Cloud Computing

Whether a large law firm or a small, boutique law firm, whether in-house counsel or a state agency, keeping up with technological advances has become a necessity for every legal department in today's world.[12] A growing number of jurisdictions are e-file friendly, and all federal district courts have defaulted to e-filing as the only permissible form of filing.[13] This has led to growth in the use of technological tools and resources that the average attorney relies on and may feel lost without. The advent of technological innovations, such as high-speed Internet connections and smaller storage and server sizes, has increased modern-day reliance on technology.[14] Today's law firms, whether big or small, private or not-for-profit, are not immune to this dependency on technology.[15] Cloud computing benefits law firms by creating worldwide accessibility and document protection while decreasing

12. Jeff Bleich & Kelly Klaus, Courting Technology Guiding New Technology Through Old Law: Expect A Few Bumps Along the Way, OR. ST. B. BULL., Dec. 1997, at 23, 28.

13. *See* E.D.N.C. CIV. R. 5.1(a)(1) ("Unless otherwise permitted by the Electronic Case Filing Administrative Policies and Procedures Manual (Policy Manual), or otherwise authorized by the assigned judge, all documents submitted for filing shall be filed electronically using the Case Management/Electronic Case Filing system (CM/ECF) and in accordance with the Policy Manual.").

14. Futeral, *supra* note 11, at 40.

15. Today's dependency on cloud services did not happen overnight; rather, these services have been a growing part of our technology usage since the early 2000s.

> If you plan to back up, share and import data, then you need access to cloud storage. The term "Cloud" storage is not new; "cloud" is a re-branding of the Web to emphasize offsite storage of information. This re-branding of the Internet began approximately in 2006 when large companies such as Google and Amazon began using "cloud computing" and "cloud storage" to describe the technological environment in which people access software and files over the Internet instead of on their desktops or company servers.
>
> The popularity of cloud storage services such as Dropbox continues to grow with the proliferation of iPhones and iPads. Because iPhones and iPads have no USB connectivity to storage devices such as thumb drives, services such as Dropbox have become an indispensable means of transferring and accessing files on iDevices. Moreover, many popular apps allow the user to link the app to Dropbox and other "cloud" storage accounts.

Id.

overall costs.[16]

1. Accessibility

Cloud computing provides attorneys with remote accessibility to any client file, document, folder, or application from anywhere with an Internet connection.[17] In fact, forty-one percent of users cite remote accessibility as the primary reason for cloud use.[18] With the development of mobile "hotspots," attorneys may access cloud services wherever they have access to a cell-phone signal, facilitating out-of-office work and access. Dropbox will also "sync" files to any other linked computers or shared folders, further facilitating out-of-office work and access.[19] This method of sharing files ensures that everyone is working with the most up-to-date copy, because it will "initiate the syncing process as soon as it determines a change has been made to the file."[20] This service allows quick and easy sharing between attorneys, paralegals, assistants, and clients.[21]

2. Safekeeping and Document Protection

Universal accessibility is merely a by-product of Dropbox's true function: backing up data off-site.[22] Cloud services, such as Amazon Web Services and Dropbox, store a user's virtual documents in remote, large-scale data centers.[23] These data centers house the servers where the data is stored, and are, according to Amazon, "housed in nondescript facilities . . . [with] extensive setback and military grade perimeter

16. Denise Penton, *Decisions On Cloud Computing Must Include Ethical Concerns*, 55 ADVOC. 40, 40 (2012) (noting that by circumventing the cost of hardware and software, the costs of maintenance and management are also avoided).

17. Kelly, *supra* note 5, at 62.

18. John Horrigan, *Use of Cloud Computing Applications and Services*, PEW INTERNET & AM. LIFE PROJECT (Sept. 12, 2008), http://pewinternet.org/Reports/2008/Use-of-Cloud-Computing-Applications-and-Services/Data-Memo.aspx.

19. *What is LAN Sync?*, DROPBOX, https://www.dropbox.com/help/137/en (last visited Nov. 15, 2013). This service facilitates sharing and syncing documents, files, folders among home desktop, laptop, and office desktop.

20. *Id.*

21. *See id.* This is an invaluable benefit, replacing the need to search an e-mail thread for the most recent version of an attached document.

22. *How Do I Sync Files Between Computers?*, DROPBOX, https://www.dropbox.com/help/4/en (last visited Nov. 15, 2013).

23. *Amazon Web Services: Overview of Security Processes*, AMAZON WEB SERVICES (Sept. 5, 2008, 5:33 PM), http://aws.amazon.com/articles/1697.

control berms as well as other natural boundary protection."[24] These super-secure data centers store multiple, and even redundant, copies of data so that in the event of a catastrophe to a user's personal storage device, such as theft, loss, or destruction, the data can be readily restored through access to a network connection.[25] These features provide Dropbox users with relief that their data is both backed up and "safe" from most physical intrusions.[26] Generally, this level of security is safe enough for the ordinary consumer using cloud computing services.[27]

3. Reducing Legal Costs

Cloud computing has dramatically reduced attorneys' costs in keeping up with ever-evolving technology.[28] Today, an attorney can outsource many traditionally internal activities to a third-party vendor.[29] Virtual Law Office Platforms, for example, offer management and marketing solutions for solo practitioners and small firms, replacing the need to employ an in-house manager or consultant.[30] Other cloud-based platforms offer solutions as well, including accounting programs, litigation management, and even e-discovery collection and review.[31] Outsourcing to third-party vendors reduces the costs associated with temporary staff during periods of high volume, and it increases consistency, all while keeping scarce office resources open for more efficient and more important tasks.[32] Monthly service subscriptions increase financial flexibility by avoiding lengthy commitments.[33] This

24. *Id.*

25. *Does Dropbox Keep Backups of my Files?*, DROPBOX, https://www.dropbox.com/help/122/en (last visited Nov. 15, 2013) ("All files synced by Dropbox are encrypted and stored securely on Amazon's Simple Storage Service (S3) over several data centers.").

26. *See id.*

27. *See id.*

28. Kelly, *supra* note 5, at 62.

29. *Id.*

30. *See, e.g.*, *About Total Attorneys*, TOTAL ATTORNEYS, http://www.totalattorneys.com/about/ (last visited Nov. 15, 2013).

31. Kelly, *supra* note 5, at 63. Specific software and platform-based cloud services include: virtual law office platforms (DirectLaw and Total Attorneys), accounting and billing programs (Bill4Time, Freshbooks, Time59, and TimeSolv), data storage and file synchronization and collaboration (Box.net, Dialawg, DropBox, JungleDisk, LiveMesh, and SugarSync), and practice management/litigation management (Clio, Credenza, Legal Workspace, LexisNexis Firm Manager, MyCase, and RealPractice). *Id.*

32. *See Pricing Terms and Conditions*, DROPBOX, https://www.dropbox.com/privacy#pricing_terms (last visited Nov. 15, 2013).

33. *See id.*

feature, common with most cloud computing service providers such as Dropbox,[34] allows law offices to pay only for the services that they need. Cloud computing provides attorneys with a risk-shifting alternative in a world where technology has become increasingly outdated and has a decreased lifespan.[35] In addition to quickly becoming obsolete, traditional set-ups are difficult to expand with the real-time needs of a modern law firm.[36]

Another valuable feature of cloud computing is its conservation of physical space. Workspace often comes at a hefty price per square foot, and in the past, this treasured commodity has been sacrificed for on-site hardware, such as physical servers and disk storage space.[37] Through the use of cloud computing services, however, law offices can transfer the burden of hosting and maintenance to a third-party cloud vendor, reducing the need for traditional computer and network set-ups.[38] By doing so, the cloud vendor becomes responsible for costs ordinarily borne by individual law offices.[39] The cost of information technology (IT) services, system updates, and maintenance are better borne by the third-party cloud vendor, which specializes in servicing many clients, rather than by the individual law firm.[40]

B. The Disadvantages of Cloud Computing

However, you cannot eat your cake and have it too![41] In other words, the great benefits of cloud computing do not come without great risks. In exchange for third-party services and maintenance, cloud users may compromise security and surrender absolute control of their data. The extent of the compromise may depend on how and where the cloud

34. *See id.*

35. *See* Daniel J. Buller & Mark H. Wittow, *Cloud Computing: Emerging Legal Issues, Data Flows, and the Mobile User*, LANDSLIDE, Nov./Dec. 2009, at 54, 54.

36. *See id.*

37. *Id.* (stating that the use of hardware and software resources required the "technical human expertise necessary to implement, maintain, and secure those resources [and that] [c]omplicated and expensive upgrade procedures were necessary to take advantage of new developments and features available for software applications").

38. *See id.* at 55.

39. *Id.*

40. *See id.* at 57. Some of the practical benefits include "pay-as-you-go" billing, the ability to subscribe only to services actually used, low upfront IT costs, the ability to expand quickly as needed, and the ability to run large applications and access large amounts of data on limited hardware. *Id.*

41. Please allow me brief literary license to reverse the order of the verbs and present the popular idiom, "You can't have your cake and eat it too" in a more logical order.

vendors store the information, and more importantly, how the cloud vendors use the information, if at all.

Surrendering control is of greater concern to attorney users of cloud computing services than to ordinary users.[42] Once an attorney user has stored his data with a cloud vendor, the attorney immediately surrenders control of the physical hardware, which houses at least one copy of the data.[43] This limits the attorney's own ability to oversee security, backup, and management of his information. Commonly, the physical locations of the cloud vendor's servers are undisclosed for security purposes, furthering uncertainty about the information's safekeeping.[44]

Physical control, however, is not the only concern. Many cloud service agreements contain nonnegotiable terms and provisions that grant the cloud vendor certain rights and licenses, while simultaneously releasing the vendor from any liability.[45] Why should these terms concern attorneys more than the general public? Although ordinary users may be concerned about their own *personal* privacy and security, attorneys must also consider the duties owed to their clients.[46] In the following Section, this Comment will survey the developing legal and ethical issues arising from attorney use of cloud computing services.

II. THE DEVELOPING LEGAL AND ETHICAL ISSUES ARISING FROM DROPBOX USE

The Model Rules of Professional Conduct (Model Rules) provide attorneys with a framework for the ethical practice of law.[47] The Model

42. Attorneys, as representatives of their clients, are necessarily held to higher standards than the general population. *See, e.g.*, N.C. RULES OF PROF'L CONDUCT pmbl. (2006) ("A lawyer, as a member of the legal profession, is a representative of clients, an officer of the legal system, and a public citizen having special responsibility for the quality of justice.").

43. *Amazon Web Services: Overview of Security Processes*, *supra* note 23.

44. *Id.* ("AWS data centers are housed in nondescript facilities[.]").

45. Buller & Wittow, *supra* note 35, at 56 ("For example, Google's license agreement for its 'Chrome' Web browser initially gave the company 'a perpetual, irrevocable, worldwide, royalty-free, and non-exclusive license to reproduce, adapt, modify, translate, publish, publicly perform, publicly display and distribute any Content which you submit, post or display on or through' the Web browser.").

46. William L. Wilson, *More on Dropbox Security*, THIRD APPLE (June 20, 2012, 7:30 AM), http://thethirdapple.wordpress.com/2012/06/20/more-on-dropbox-security/ (suggesting that Dropbox's security and privacy policy may be adequate for "routine client data and documentation," but not for more "sensitive client information").

47. *See* MODEL RULES OF PROF'L CONDUCT pmbl. (1983).

Rules also attach duties when an attorney-client relationship exists.[48] The American Bar Association provides guidance "in legal ethics and professional responsibility through the adoption of professional standards that serve as models of the regulatory law governing the legal profession."[49] Three Model Rules are primarily implicated in an attorney's use of cloud computing services: Rule 1.1: Competence, Rule 1.6: Confidentiality of Information, and Rule 5.3: Responsibilities Regarding Nonlawyer Assistant.

The American Bar Association created the ABA Commission on Ethics 20/20 (ABA Commission) to "develop guidance for lawyers regarding their ethical obligations to protect [confidential client] information when using technology, and to update the Model Rules of Professional Conduct to reflect the realities of a digital age."[50] The ABA Commission recognized that technology has integrated itself into and has evolved the practice of law.[51] Technology affects the manner in which attorneys deliver legal services, communicate with clients, store confidential client information, and even conduct investigation and discovery.[52] Because of this shift in the legal practice, new ethical issues arise relating specifically to an attorney's duty to protect confidential information.

After three years of studies, submissions, and commentary, the ABA Commission submitted two separate recommendations to the ABA.[53] First, the ABA Commission recommended that the ABA create a regularly updated website that provides attorneys with specific and timely guidance regarding their use of technology, such as cloud computing services, that may affect attorneys' duty of confidentiality.[54] Second, the ABA recommended amending several Model Rules and their

48. *Id.*

49. *See* MODEL RULES OF PROF'L CONDUCT preface.

50. ABA COMMISSION ON ETHICS 20/20, HOUSE OF DELEGATES FILINGS: RESOLUTION AND REPORT: TECHNOLOGY & CONFIDENTIALITY, 1, (Aug. 2012), http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/2012_hod_annual_meeting_105a_filed_may_2012.authcheckdam.pdf.

51. ABA COMMISSION ON ETHICS 20/20, HOUSE OF DELEGATES FILINGS: INTRODUCTION, 4–5, (Aug. 2012), http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/20120508_ethics_20_20_final_hod_introdution_and_overview_report.authcheckdam.pdf.

52. *Id.*

53. ABA COMMISSION ON ETHICS 20/20, HOUSE OF DELEGATES FILINGS: RESOLUTION AND REPORT: TECHNOLOGY & CONFIDENTIALITY, *supra* note 50, at 1.

54. *Id.*

official comments.[55] In August 2012, the ABA Commission did in fact amend several Model Rules and official comments. Three of at least twelve amendments affected the aforementioned Model Rules or their comments that relate to the duty of confidentiality.[56]

Although every jurisdiction had adopted some form of the Model Rules or their comments as of January 1, 2010,[57] only Delaware has adopted the ABA Commission on Ethics 20/20 August 2012 amendments (August 2012 amendments) in full or in part.[58] In considering the potential consequences of not adopting the August 2012 amendments, North Carolina serves as a suitable illustration because the North Carolina State Bar does not currently appear to be considering the adoption of such amendments.[59]

Before going forward, this Comment will briefly introduce the North Carolina State Bar. An attorney practicing in North Carolina necessarily becomes a member of the North Carolina State Bar.[60] The North Carolina State Bar oversees the administration and enforcement of the North Carolina Rules of Professional Conduct (N.C. Rules). The

55. *Id.*

56. The aforementioned Model Rules, Rules 1.1, 1.6, and 5.3, are the emphasis of this Comment because of their impact on an attorney's usage of the cloud regarding the duty of confidentiality.

57. *See generally State Adoption of the ABA Model Rules of Professional Conduct and Comments*, ABA (May 23, 2011), http://www.americanbar.org/content/dam/aba/migrated/cpr/pic/comments.authcheckdam.pdf.

58. *Variations of the ABA Model Rules of Professional Conduct: Rule 1.6: Confidentiality of Information*, ABA 4 (Aug. 16, 2013), http://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/mrpc_1_6.authcheckdam.pdf; *Variations of the ABA Model Rules of Professional Conduct: Rule 5.3 Responsibilities Regarding Nonlawyer Assistance*, ABA 2 (Aug. 16, 2013), http://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/mrpc_5_3.authcheckdam.pdf.

59. The North Carolina State Bar has not yet adopted the ABA Commission on Ethics 20/20 August 2012 amendments, nor has it proposed to adopt such amendments. *See States Making Amendments to the Model Rules of Professional Conduct Dates of Adoption*, ABA, http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/chrono_list_state_adopting_model_rules.html (last visited Nov. 15, 2013) (adopting Model Rules in part on March 1, 2003); *Proposed Rule Amendments*, N.C. STATE BAR (July 2013), http://www.ncbar.com/rules/proprul.asp.

60. *See* N.C. GEN. STAT. § 84-4 (2011) ("Persons other than members of State Bar prohibited from practicing law."); *see also* 27 N.C. ADMIN. CODE 01A .0201(b) (2008) ("The active members shall be all persons who have obtained licenses entitling them to practice law in North Carolina, including persons serving as justices or judges of any state or federal court in this state, unless classified as inactive members by the council.").

N.C. Rules are fundamentally shaped by the Model Rules. Every licensed North Carolina attorney, as an individual member of the profession, is responsible for the promotion of the profession's standing and reputation.[61] The North Carolina State Bar Ethics Committee (Ethics Committee) periodically provides ethical guidance on issues of professional conduct, which are formalized as Formal Ethics Opinions, and later published by the North Carolina State Bar. Formal Ethics Opinions serve as guiding principles for interpreting the N.C. Rules.[62] An analysis of the August 2012 amendments and their effect on an attorney's duty of confidentiality is presented next.

A. Rule 1.1: Competence

1. Model Rule 1.1

The Model Rules require attorneys to provide competent representation for their clients.[63] The ever-evolving nature of cloud computing, and technology generally, makes it important for attorneys to stay informed of the changes in relevant technology, and to be aware of how those changes may affect their representation. The Model Rules' comments to Rule 1.1 direct attorneys to stay well-informed and up-to-date on both changes in the law and changes in the "benefits and risks associated with [] technology."[64] Although the comments to the Model Rules alone do not impose a duty on attorneys to stay abreast of the relevant changes in technology, they should serve as guidelines for attorneys to follow in maintaining competent representation.

61. N.C. RULES OF PROF'L CONDUCT pmbl. ¶¶ 14–17 (2006).

62. 27 N.C. ADMIN. CODE 01D .0101(j) (2004) ("'Formal ethics opinion' shall mean a published opinion issued by the council to provide ethical guidance for attorneys and to establish a principle of ethical conduct.").

63. MODEL RULES OF PROF'L CONDUCT R. 1.1 (1983) ("A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.").

64. *Id.* cmt. 8 ("To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.").

2. N.C. Rule 1.1

The N.C. Rules are silent on directing attorneys to stay abreast of the relevant changes in technology.[65] A North Carolina attorney, therefore, may not think to consider changes in technology as affecting his ability to competently represent his clients.[66] When an attorney engages in the active use of cloud computing services, however, it is important that he maintain an appropriate level of education regarding cloud computing and its effect on his clients. As such, the ABA rightfully chose to make explicit an attorney's duty of competence with technology, and given what is at stake, North Carolina should make the duty explicit as well.[67]

B. Rule 1.6: Confidentiality of Information

1. Model Rule 1.6

The Model Rules impose a duty of confidentiality in attorney-client relationships that requires attorneys to take affirmative steps to protect confidential client information.[68] Model Rule 1.6 further requires attorneys to "make reasonable efforts to prevent the inadvertent or

65. N.C. RULES OF PROF'L CONDUCT R. 1.1 ("Competent representation requires the legal knowledge, skill, thoroughness, and preparation reasonably necessary for the representation."). Although there is no explicit duty that an attorney understand basic features of relevant technology, as in the ABA Commission's amended Model Rule 1.1, the general expectation and obligation that an attorney act competently in the representation of a client is echoed in the N.C. Rules' preamble:

> In all professional functions a lawyer should be competent, prompt, and diligent. A lawyer should maintain communication with a client concerning the representation. A lawyer should keep in confidence information relating to representation of a client except so far as disclosure is required or permitted by the Rules of Professional Conduct or other law.

N.C. RULES OF PROF'L CONDUCT pmbl. ¶ 4. This general expectation and obligation can be read broadly to include a duty to maintain a competent level of awareness regarding technology that affects a law practice.

66. Although the duty to maintain competence regarding the benefits and risks associated with technology has not been formally adopted in the N.C. Rules, the North Carolina State Bar Ethics Committee recently forewarned that attorneys must "act competently to safeguard information" shared with SaaS providers. N.C. STATE BAR, 2011 Formal Ethics Op. 6 (2012).

67. ABA COMMISSION ON ETHICS 20/20, HOUSE OF DELEGATES FILINGS: INTRODUCTION, *supra* note 51, at 8.

68. MODEL RULES OF PROF'L CONDUCT R. 1.6.

unauthorized disclosure of [client information]."[69] Thus, under Model Rule 1.6, an attorney has a duty to safeguard confidential client information that he turns over to cloud vendors for cloud services. The Model Rules demand this protection because once confidential information has been compromised or exposed to the public, there is no way to make the information confidential again. The importance and vulnerability of confidential information means that an attorney must take greater measures to protect against the inadvertent disclosure of client information, compared to those measures he may use for his own personal information. This need for greater protective measures is included in the comments to Model Rule 1.6, which indicate that an attorney "*must* take reasonable precautions to prevent [confidential client] information from coming into the hands of unintended recipients."[70]

Model Rule 1.6 requires that attorneys act reasonably in protecting their clients' confidential information, and it shields those who have acted accordingly from a potential breach of the duty of confidentiality.[71] Additionally, comment 18 to Model Rule 1.6 provides that "inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of [the duty of confidentiality] if the lawyer [] made reasonable efforts to prevent the access or disclosure."[72] Comment 18 further determines the reasonableness of an attorney's efforts by considering: "the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients."[73]

In today's technology-driven world, an attorney routinely surrenders control of confidential information in ordinary transmissions and communications.[74] As a result, there are several security concerns that may implicate a breach of the duty of confidentiality. Most notably, the cloud vendor or an unknown third party may gain unauthorized access to the information.[75] The Model Rules, however, may insulate an

69. *Id.* R. 1.6(c).

70. *Id.* cmt. 19 (emphasis added).

71. *Id.* cmt. 18.

72. *Id.*

73. *Id.*

74. For example, attorneys regularly send confidential information intra-office or to clients via e-mails, as well as store redundant copies of client files in cloud storage.

75. *See* Hume, *supra* note 7, at 53–54.

attorney against a potential breach of the duty of confidentiality where that attorney has made reasonable efforts to prevent against unauthorized access or inadvertent disclosure.[76] This provision in the Model Rules protects an attorney against the intentional misuse of confidential information by a cloud vendor and protects an attorney from the interception of such information by an unknown third party.[77] Thus, absent the Model Rules' provisions for "reasonable efforts" in preventing disclosure, an attorney may be liable for a breach of the duty of confidentiality.

2. N.C. Rule 1.6

The Model Rules require that an attorney make "reasonable efforts" to prevent inadvertent or unauthorized disclosure,[78] and they protect an attorney who has done so,[79] whereas the N.C. Rules are silent in the same regard.[80] The N.C. Rules impose a similar duty of confidentiality on attorneys regarding the protection of confidential client information.[81] An attorney "must act competently to safeguard [confidential client] information against inadvertent or unauthorized disclosure"[82] and "take reasonable precautions to prevent the information from coming into the hands of unintended recipients."[83] However, the N.C. Rules, in contrast to the Model Rules, do not enumerate comparable protections for inadvertent disclosure.[84] Here, the N.C. Rules merely offer that an attorney should "act competently" and "take reasonable precautions" to prevent inadvertent disclosures, but they do not provide guidelines on how to act accordingly.[85] This means that an inadvertent or unauthorized disclosure, therefore, may be a breach of the duty of confidentiality under the N.C. Rules, even if the attorney has made *reasonable* efforts to prevent such disclosure.

---

76. MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. 18.

77. *Id.* Whether it is a prying competitor, or a rogue employee of the cloud vendor, the attorney is not liable.

78. *Id.* R. 1.6(c).

79. *Id.* cmt. 18.

80. *See id.* R. 1.6(c); *but cf.* N.C. RULES OF PROF'L CONDUCT R. 1.6 (2003).

81. *See* N.C. RULES OF PROF'L CONDUCT R. 1.6 ("[U]nless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by paragraph (b).").

82. *Id.* cmt. 17.

83. *Id.* cmt. 18.

84. *See id.* (safeguarding attorneys who have made a reasonable effort to prevent inadvertent or unauthorized disclosure).

85. *See id.* cmts. 17–18.

Recently, the Ethics Committee addressed cloud usage by attorneys.[86] In the opinion, the Ethics Committee concluded that an attorney may use cloud computing services "if *reasonable care* is taken to minimize the risks of inadvertent disclosure of confidential information and to protect the security of client information and client files."[87] In an analogous opinion sixteen years earlier, the Ethics Committee decided that at a minimum, attorneys "must take steps to minimize the risks that confidential information may be disclosed," but attorneys are not required to "use only infallibly secure methods of communication."[88] Accordingly, it appears that a North Carolina attorney must act competently, reasonably precautious, and with reasonable care when contracting with a cloud vendor. However, an attorney in North Carolina is left without the protection of Model Rule 1.6(c) as well as the factors for determining "reasonable efforts" under Model Rule 1.6, comment 18.

C. Rule 5.3: Responsibilities Regarding Nonlawyer Assistant

1. Model Rule 5.3

The duty of confidentiality prohibits attorneys from disclosing "information relating to the representation of a client unless . . . the disclosure is impliedly authorized in order to carry out the representation."[89] Under Model Rule 5.3, cloud vendors retained by an attorney fall within the category of nonlawyer assistant, and thus, disclosure to a cloud vendor may be exempt from the prohibition against disclosing confidential client information.[90] Although an attorney may disclose ordinarily nondisclosable information to a cloud vendor, he must make "reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that the [cloud vendor's] conduct

86. *See* 2011 Formal Ethics Op. 6, *supra* note 66 (opining that an attorney "may contract with a vendor of software as a service [i.e., cloud vendor] provided the lawyer uses reasonable care to safeguard confidential client information").

87. *Id.* (emphasis added).

88. N.C. STATE BAR, RPC 215 (1995) (answering an inquiry regarding the use of unsecure methods of communication for the transmission of confidential client information).

89. MODEL RULES OF PROF'L CONDUCT R. 1.6(a) (1983).

90. MODEL RULES OF PROF'L CONDUCT R. 5.3 cmt. 3 (including "using an Internet-based service to store client information," among others in a demonstrative list of non-attorney assistants outside the firm).

is compatible with the professional obligations of the lawyer."[91] Thus, the attorney must approve of the policies and procedures used by the cloud vendor, and he must confirm that those policies and procedures align with his own professional standards.[92]

As if on cue, the Model Rules also provide direction in determining when reasonable efforts have been made.[93] What constitutes a reasonable effort will vary depending on the circumstances. Therefore, comment 3 to Rule 5.3 includes factors to consider when determining the extent of an attorney's duty to make "reasonable efforts" to ensure that a cloud vendor's practices align with his own practices.[94] The Model Rules contemplate four such factors, including: "the education, experience and reputation of the nonlawyer; the nature of the services involved; the terms of any arrangements concerning the protection of client information; and the legal and ethical environments of the jurisdictions in which the services will be performed, particularly with regard to confidentiality."[95]

Although the Model Rules' comment does not objectively direct what efforts an attorney *must* take, the factors help guide the inquiry in determining whether the attorney's efforts were reasonable, given the circumstances at hand.[96]

2. N.C. Rule 5.3

Under N.C. Rule 5.3, an attorney has nearly identical obligations regarding a nonlawyer assistant as those obligations under Model Rule 5.3.[97] An attorney in North Carolina must "effect measures giving reasonable assurance" that the cloud vendor will act in a manner

91. *Id.* R. 5.3(a).

92. *See* H. Ward Classen, *Cloudy with a Chance of Rain: Avoiding Pitfalls in Cloud Computing*, 45 MD. B.J., July/Aug. 2012, at 18, 21–22; *see also* Louise Lark Hill, *Cloud Nine or Cloud Nein? Cloud Computing and its Impact on Lawyers' Ethical Obligations and Privileged Communications*, 2013 PROF. LAW. 109, 113 (2013) (asserting that "there are many contracting models under which cloud services are offered, the competent lawyer must select the appropriate model, which necessitates understanding the risks inherent in the use of cloud computing").

93. *See* MODEL RULES OF PROF'L CONDUCT R. 5.3 cmt. 3.

94. *Id.*

95. *Id.*

96. *Id.*

97. *See* N.C. RULES OF PROF'L CONDUCT R. 5.3 (2003); *see also* MODEL RULES OF PROF'L CONDUCT R. 5.3.

consistent with the attorney's obligations of confidentiality.[98] Although the N.C. Rules do not set standards for reasonable efforts, the Ethics Committee recommends that an attorney reach "an agreement on how the vendor will handle confidential client information in keeping with the [attorney's] professional responsibilities."[99] Although the Ethics Committee repeats in the same opinion that there should be a "[c]areful review of the terms of the law firm's user or license agreement with the [cloud] vendor including the security policy," the Ethics Committee fails to include guiding principles for such an agreement.[100]

III. THE PRACTICAL EFFECTS OF THE ABA COMMISSION ON ETHICS 20/20 AMENDMENTS ON ATTORNEY USAGE OF DROPBOX AND SIMILAR CLOUD SERVICE PROVIDERS

This Section considers Dropbox usage in jurisdictions that both have and have not adopted the August 2012 amendments. Each amendment is considered individually when contemplating whether the duties set forth may be violated by using Dropbox. Finally, each Subsection contains a recommendation for both jurisdictions that have and have not adopted the August 2012 amendments in an effort to better guide an attorney in his use of cloud computing services.

Dropbox boasts that it serves over 200 million users.[101] Dropbox's freemium-style hosting services offer cloud storage and file synchronization, and these services are quickly becoming the standard in cloud storage.[102] Dropbox is popular with professional and non-professional users alike.[103] Due to their ethical obligations, attorneys should have some reservations about using Dropbox and other similar services in their practice. Below, this Comment explores the practical effects of the adoption and non-adoption of the August 2012 amendments as they relate to the use of Dropbox and other similar cloud services.

The August 2012 amendments create several duties, including the duty to make "reasonable efforts to prevent the inadvertent or

98. N.C. RULES OF PROF'L CONDUCT R. 5.3(a) ("[A] lawyer . . . shall make reasonable efforts to ensure that the firm or organization has in effect measures giving reasonable assurance that the nonlawyer's conduct is compatible with the professional obligations of the lawyer[.]").

99. 2011 Formal Ethics Op. 6, *supra* note 66.

100. *Id.*

101. *About Dropbox*, *supra* note 8.

102. *See id.*

103. Futeral, *supra* note 11, at 40.

unauthorized disclosure of" confidential client information,[104] to provide "competent representation,"[105] and to "effect measures" in the employment of cloud vendors to ensure that such vendors act in accordance with the professional responsibilities of the attorney.[106]

A. Rule 1.6: Confidentiality of Information

Model Rule 1.6(c) requires that an attorney "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of" confidential client information.[107] Reasonable efforts, however, are determined by fact-intensive, subjective factors that may depend on the circumstances. For that reason, this Comment now considers Dropbox's policies and procedures.

A basic security method employed by most cloud vendors is encryption.[108] This Comment's principal illustration, Dropbox, encrypts all files stored on its servers using the AES-256 standard by default,[109] which Dropbox states is "the same encryption standard used by banks to secure customer data."[110] In laymen's terms, the data uploaded is secured with a "key," and without the key, any data retrieved will appear as incomprehensible gibberish.[111] Thus, storing encrypted client data is much like securing paper files under lock-and-key.[112] In the same manner that a physical lock-and-key is vulnerable to theft by a burglar and a crowbar, a dedicated and knowledgeable cyber-thief can likewise access encrypted files.[113] Lacking a digital crowbar, cyber-thieves can access encrypted data through the encryption keys by exploiting

104. MODEL RULES OF PROF'L CONDUCT R. 1.6(c) (1983).

105. MODEL RULES OF PROF'L CONDUCT R. 1.1. Comment 8 specifies that to remain competent, an attorney should "keep abreast of changes in the law and its practice." *Id.* cmt. 8.

106. MODEL RULES OF PROF'L CONDUCT R. 5.3.

107. MODEL RULES OF PROF'L CONDUCT R. 1.6(c).

108. AES CRYPT, http://www.aescrypt.com/ (last visited Nov. 16, 2013).

109. If this terminology is beyond your understanding, likely, you are not alone. AES is a file encryption software that "uses the industry standard Advanced Encryption Standard (AES) to easily and securely encrypt files." *Id.*

110. *Security Overview*, DROPBOX, https://www.dropbox.com/security/ (last visited Nov. 16, 2013).

111. Wilson, *supra* note 46.

112. Tomasz Stasiuk, *Is Cloud Storage Secure Enough For Lawyers?*, THE MAC LAWYER (Sept. 27, 2010), http://www.themaclawyer.com/2010/09/software/guest-post-is-cloud-storage-secure-enough-for-lawyers/.

113. *Encrypt Or Not? Things You Should Consider*, CERBERUS SYSTEMS, INC., http://www.cerberussystems.com/INFOSEC/consider.htm (last visited Nov. 16, 2013).

operator error or simply by gaining access to the administrator's "keys."[114]

Remotely storing redundant backup copies of confidential client files may be a good practice in order to prevent loss of sensitive and important files. Using Dropbox, however, may not be the ideal way to do so. Although Dropbox encrypts the data that is uploaded to its servers, it unnecessarily maintains the encryption keys.[115] While Dropbox's primary function, storage and backup, should not necessitate access to unencrypted files, its secondary function, file synchronization, however, does require access to unencrypted files.[116] Therefore, using Dropbox is inconsistent with an attorney's duty to use reasonable efforts to prevent inadvertent or unauthorized disclosure because unencrypted files, transmitted through unsecured networks, are vulnerable to theft or misuse.[117]

The lack of guidance in the ever-growing field of cloud computing services can potentially be remedied by looking to the ABA Commission's recommendations.[118] Widespread adoption of the August 2012 amendments to Rule 1.6 and its comments would reinforce an attorney's ethical duty to take reasonable efforts to prevent the inadvertent disclosure of confidential client information, regardless of

114. *See id.* ("How can high-grade encryption be cracked? By definition, it can't be—but its keys can.").

115. *Security Overview*, *supra* note 110.

116. For more information on file synchronization and its inconsistency with proper encryption, see Christopher Soghoian, *How Dropbox Sacrifices User Privacy for Cost Savings*, SLIGHT PARANOIA (Apr. 12, 2011, 1:00 PM), http://paranoia.dubfire.net/2011/04/how-dropbox-sacrifices-user-privacy-for.html.

117. Recently, the North Carolina Business Court stepped into the field of attorney-client privilege to define the privilege's boundaries regarding inadvertent disclosure. The court found a waiver of the attorney-client privilege where an attorney did not take "reasonable efforts adequate to protect against a waiver[.]" Blythe v. Bell, 2012 NCBC LEXIS 44, at *31 (N.C. Super. Ct. July 26, 2012). *See also* J.D. Hensarling, *Inadvertent Waiver of the Attorney-Client Privilege in E-discovery Cases under North Carolina Law—Does North Carolina Need a Rule 502?*, CAMPBELL LAW OBSERVER (Aug. 20, 2012), http://campbelllawobserver.com/2012/08/inadvertent-waiver-of-the-attorney-client-privilege-in-e-discovery-cases-under-north-carolina-law-does-north-carolina-need-a-rule-502/ ("Defendants' failure to employ reasonable precautions to avoid disclosure was so egregious that it was unnecessary to go through each of the five elements of the balancing test."). Although the *Blythe v. Bell* opinion deals primarily with the waiver of the attorney-client privilege through e-discovery, the essence of the opinion remains relevant to issue of the duty of confidentiality in using cloud computing services.

118. ABA COMMISSION ON ETHICS 20/20, HOUSE OF DELEGATES FILINGS: RESOLUTION AND REPORT: TECHNOLOGY & CONFIDENTIALITY, *supra* note 50, at 1.

the medium used.[119] Currently, Delaware remains the lone state to have adopted in full the ABA Commission's August 2012 amendments concerning the safeguarding of confidential client information.[120]

Additionally, individual states should adopt a uniform standard of best practices for attorney use of cloud services. In 2011, the International Legal Technology Standards Organization (ILTSO), a non-profit organization, announced standards for the use of technology and cloud services in law practice.[121] This Comment uses the standards proposed by the ILTSO for illustrative purposes only in determining potential best practices. The ILTSO recommends that data that is stored on cloud servers should be access-controlled at every point, thereby only allowing access to unencrypted data to intended parties via a properly maintained login and password combination.[122] In between point A and point B, however, data should be encrypted at every point. Therefore, end-to-end encryption should be required in order to prevent plain text data from being sent over unsecured connections.[123]

B. Rule 1.1: Competence

Dropbox and similarly modeled cloud service providers may rob attorneys of the opportunity to zealously and competently represent

---

119. *See* MODEL RULES OF PROF'L CONDUCT R. 1.6(c) (1983).

120. *Variations of the ABA Model Rules of Professional Conduct: Rule 1.6: Confidentiality of Information*, *supra* note 58.

121. International Legal Technical Standards Organization, 2011 Guidelines for Legal Professionals 2 (2011) (unpublished manuscript) (on file with the Campbell Law Review) [hereinafter ILTSO 2011 Guidelines] ("The mission of the International Legal Technical Standards Organization is to develop and promote secure and ethically-conscious technology standards within the legal profession.").

122. *Id.* at 14.

123. *Id.* at 15. For the more technologically sophisticated, ILTSO goes on to describe the appropriate levels of encryption:

> Unencrypted movement of data "packets" across the Internet present an unacceptable risk to *client data* . . . . Therefore, a minimum of 128-bit *SSL or TLS* encryption should be required for every browser and email client connection, which should be verifiable by an unexpired *third party certificate* with *extended validation*. For file transfer protocol transmissions (FTP), only SFTP or FTPS (the encrypted variants) should be utilized. Note that secure socket layer (*SSL*)-enabled email does not ensure end-to-end *encryption* of e-mail data, since the transmission may travel over unencrypted links before reaching the recipient.

Id.

their clients, as required by the rules of professional conduct.[124] Under both the Model Rules and the N.C. Rules, Rule 1.1, in conjunction with Rule 1.6, requires attorneys to act competently in preserving confidentiality in communications made in the scope of representation.[125] The duty of confidentiality, however, is not absolute, as confidential information is subject to enumerated exceptions in both the Model Rules and the N.C. Rules.[126] Both the Model Rules and the N.C. Rules state that an attorney may reveal confidential information to the extent that the attorney believes is necessary in order to comply with other law or court order.[127] This exception, however, does not require that an attorney mindlessly comply with any request for production, even in the context of court orders.[128] Here, because an attorney's discretion to reveal confidential information is only to the extent that the attorney believes is necessary, the attorney has an ethical obligation to object on legitimate grounds to the court order, either to the order's

124. MODEL RULES OF PROF'L CONDUCT R. 1.1; N.C. RULES OF PROF'L CONDUCT R. 1.1 (2003).

125. Both the Model Rules and the N.C. Rules require attorneys to provide "[c]ompetent representation" and to "not reveal information acquired during the professional relationship." *See* MODEL RULES OF PROF'L CONDUCT R. 1.1, 1.6(a); N.C. RULES OF PROF'L CONDUCT R. 1.1, 1.6(a).

126. MODEL RULES OF PROF'L CONDUCT R. 1.6(b); N.C. RULES OF PROF'L CONDUCT R. 1.6(b). The N.C. Rules allow an attorney to disclose confidential information for the following reasons:

> (1) to comply with the Rules of Professional Conduct, the law or court order;
>
> (2) to prevent the commission of a crime by the client;
>
> (3) to prevent reasonably certain death or bodily harm;
>
> (4) to prevent, mitigate, or rectify the consequences of a client's criminal or fraudulent act in the commission of which the lawyer's services were used;
>
> (5) to secure legal advice about the lawyer's compliance with these Rules;
>
> (6) to establish a claim or defense on behalf of the lawyer in a controversy between the lawyer and the client; to establish a defense to a criminal charge or civil claim against the lawyer based upon conduct in which the client was involved; or to respond to allegations in any proceeding concerning the lawyer's representation of the client; or
>
> (7) to comply with the rules of a lawyers' or judges' assistance program approved by the North Carolina State Bar or the North Carolina Supreme Court.

N.C. RULES OF PROF'L CONDUCT R. 1.6(b). The Model Rules version of Rule 1.6 provides a list of similar reasons. *See* MODEL RULES OF PROF'L CONDUCT R. 1.6(b).

127. MODEL RULES OF PROF'L CONDUCT R. 1.6(b)(6); *see also* N.C. RULES OF PROF'L CONDUCT R. 1.6(b)(1).

128. *See* MODEL RULES OF PROF'L CONDUCT R. 1.6(b)(6); *see also* N.C. RULES OF PROF'L CONDUCT R. 1.6(b)(1).

entirety or to the order's scope.[129] Both the Model Rules and the N.C. Rules make this duty clear in comment 15 and comment 14, respectively, to Rule 1.6. The Model Rules specify that:

> A lawyer may be ordered to reveal information relating to the representation of a client by a court or by another tribunal or governmental entity claiming authority pursuant to other law to compel the disclosure. Absent informed consent of the client to do otherwise, the lawyer should assert on behalf of the client all nonfrivolous claims that the order is not authorized by other law or that the information sought is protected against disclosure by the attorney-client privilege or other applicable law.[130]

This duty to challenge court orders and other requests for confidential information is echoed in the preamble to the Model Rules, stating that "it is a lawyer's duty, when necessary, to challenge the rectitude of official action."[131] Thus, both the Model Rules and the N.C. Rules make it clear that court orders or requests for production of confidential client information should be vigorously challenged.

An attorney's duty to challenge and object is in conflict with Dropbox's policies. Each cloud vendor, be it Google Drive, iCloud, or Dropbox, authors its own terms of service and privacy policy. Cloud vendors, therefore, have the discretion to set lax policies concerning the disclosure of user data under threat of court order or subpoena, because by virtue of their own policies, the vendors are under no duty to inform users that their data and information has been seized through a court order or through a subpoena.[132] The Dropbox privacy policy should be

---

129. MODEL RULES OF PROF'L CONDUCT R. 1.6(b); N.C. RULES OF PROF'L CONDUCT R. 1.6(b). Before challenging any court order or subpoena, the attorney should consult with the client and determine whether the client consents to the disclosure. *See* N.C. RULES OF PROF'L CONDUCT R. 1.6(a).

130. MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. 15. The N.C. Rules include a similar provision in comment 14:

> Paragraph (b)(1) also permits compliance with a court order requiring a lawyer to disclose information relating to a client's representation . . . . [H]owever, the lawyer must, absent informed consent of the client to do otherwise, assert on behalf of the client all nonfrivolous claims that the information sought is protected against disclosure by the attorney-client privilege or other applicable law.

N.C. RULES OF PROF'L CONDUCT R. 1.6 cmt. 14.

131. MODEL RULES OF PROF'L CONDUCT pmbl. ¶ 5.

132. *See Privacy Policy*, GOOGLE POLICIES & PRINCIPLES (June 24, 2013), http://www.google.com/intl/en/policies/privacy/ (stating that "we will share personal information with companies, organizations or individuals outside of Google if we have a good-faith belief that access, use, preservation or disclosure of the information is

specifically alarming to an attorney that currently uses or is considering using Dropbox for backup and storage of his client files.[133] The most recent privacy policy published by Dropbox includes a subsection titled, "Compliance with Laws and Law Enforcement Requests; Protection of Dropbox's Rights," which declares that:

> [Dropbox] may disclose to parties outside Dropbox files stored in your Dropbox and information about you that we collect when we have a good faith belief that disclosure is reasonably necessary to (a) *comply with a law, regulation or compulsory legal request*; (b) protect the safety of any person from death or serious bodily injury; (c) prevent fraud or abuse of Dropbox or its users; or (d) to protect Dropbox's property rights. If we provide your Dropbox files to a law enforcement agency as set forth above, *we will remove Dropbox's encryption from the files* before providing them to law enforcement.[134]

Dropbox does not protect attorney-client confidentialities. Instead, Dropbox surrenders unencrypted, protected communications upon any request that Dropbox deems legally compulsory.[135] This policy, which may not affect the decisions of an ordinary user, deprives an attorney's client of legal rights and jeopardizes an attorney's competent representation. A hint of paranoia and creativity may lead one to consider the catastrophic implications of storing proprietary files on cloud-based storage where "a corporate competitor might attempt to use a subpoena to force a cloud storage service to disclose sensitive files."[136]

It is imperative that an attorney who contracts with cloud vendors is afforded notice of court orders or subpoenas due to his ethical obligation to challenge and to attempt to limit disclosure.[137] Without

---

reasonably necessary to: meet any applicable law, regulation, legal process or enforceable governmental request"); *Privacy Policy*, APPLE (Aug. 1, 2013), http://www.apple.com/privacy/ (disclosing personal information when deemed necessary "by law, legal process, litigation, and/or requests from public and governmental authorities *within or outside* your country of residence").

133. *See* Wilson, *supra* note 46 (suggesting that Dropbox's security and privacy policy may be adequate for "routine client data and documentation," but not for more "sensitive client information").

134. *Dropbox Privacy Policy*, DROPBOX (Apr. 10, 2013), https://www.dropbox.com/privacy (emphasis added).

135. *Id.* In its privacy policy, Dropbox does not include how it determines valid "legal requests."

136. Alan W. Krantz, *Attorney-Client Privilege in the Cloud*, MBHB SNIPPETS, Summer 2011, at 1, 12 (suggesting that rival, business or otherwise, may find cloud vendors as a more susceptible gatekeeper to sensitive information).

137. *See* MODEL RULES OF PROF'L CONDUCT R. 1.6(b) (1983); N.C. RULES OF PROF'L CONDUCT R. 1.6(b) cmt. 14 (2003).

proper notice of a court order or subpoena, proper objections available to the client and to the attorney will fail to be asserted—and without proper objections to court orders and subpoenas, it can hardly be said that an attorney is exercising competent representation.[138] Where the Model Rules require an attorney to stay well-informed of the relevant changes in technology that affect his law practice, the N.C. Rules do not make explicit that same duty.[139]

Here, adoption of the ABA Commission's amendments to Rule 1.1 and its comments would make the duty to stay abreast of changes in the law and its practice as they pertain to the benefits and risks associated with relevant technology explicit, whereas the ethical rules in the remaining forty-nine states have failed to do so.[140] The ILTSO recommends cloud backup and storage generally; unlike local backups, cloud storage is protected from local system failures and local physical catastrophe.[141] Another standard of best practices may be the adoption of a uniform cloud user agreement that provides notification to users when their data is under threat of court order or subpoena.

C. Rule 5.3: Responsibilities Regarding Nonlawyer Assistant

Model Rule 5.3 governs an attorney's retention of a non-attorney and directs that the attorney must "make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that the person's conduct is compatible with the professional obligations of the lawyer."[142] The attorney's professional obligations stem from the previously discussed duty of confidentiality set forth in Model Rule 1.6. The amended comments to Model Rule 5.3 alert an attorney of his duty

138. Also, consider the collateral consequences of an attorney not objecting to a court order or subpoena, such as a waiver of right to appeal or an action for malpractice.

139. N.C. Rule 5.3 does, however, address establishing "measures giving reasonable assurance that the nonlawyer's conduct is compatible with the professional obligations of the lawyer." N.C. RULES OF PROF'L CONDUCT R. 5.3. The duty in N.C. Rule 5.3 requires a North Carolina attorney to be well-informed of the cloud vendor's policy to ensure that such policy is in accord with the attorney's professional obligations. The N.C. Rules, however, do not require the same duties as the amended Model Rule 1.1 demands. *See* MODEL RULES OF PROF'L CONDUCT R. 1.1.

140. MODEL RULES OF PROF'L CONDUCT R. 1.1. Again, Delaware is the only state to have adopted the August 2012 amendments. *See Order Amending Rules 1.0, 1.1, 1.4, 1.6, 1.17, 1.18, 4.4, 5.3, 5.5, 7.1, 7.2 and 7.3*, DEL. LAWYERS' RULES OF PROF'L CONDUCT, 8 (Jan. 15, 2013), *available at* http://courts.delaware.gov/Rules/dlrpc2013rulechange.pdf (amending, *inter alia*, Delaware Lawyers' Rules of Professional Conduct Rule 1.1, comment 8).

141. ILTSO 2011 Guidelines, *supra* note 121, at 17.

142. MODEL RULES OF PROF'L CONDUCT R. 5.3(a).

to give intelligible standards and instructions to retained non-attorneys outside the firm that are cloud vendors.[143] Thus, an attorney must require that his non-attorney cloud service providers respect the duty of confidentiality that the attorney owes to his clients. More specifically, Model Rule 1.6 and Model Rule 5.3 together require that an attorney has reasonable assurance from cloud vendors that the cloud vendors will make reasonable efforts to prevent the inadvertent or unauthorized disclosure of confidential client information.[144]

By default, Dropbox encrypts the files and the data stored on its servers, and therefore, Dropbox has access to all of the files and all of the data stored because it holds the keys to the encrypted data.[145] Dropbox admits that its employees are able to access user data for reasons stated in its privacy policy—namely subpoenas and court orders.[146] Dropbox claims it rarely accesses personal user data, however, the service operates on a model that de-duplicates the files that have been previously stored online.[147] This model saves Dropbox valuable storage space by only storing a single copy of a file whenever two or more different users have stored the same single file in their respective accounts.[148] It follows, then, that Dropbox must routinely access personal user data to the extent necessary to detect files already uploaded to its storage servers. This necessarily means that Dropbox has access to a user's unencrypted data at all times, not only in limited situations as it claims, otherwise, it would be unable to detect duplicate data stemming from different user accounts.[149]

Recall that under Model Rule 5.3 an attorney must "effect measures giving reasonable assurance that the [cloud vendor]'s conduct is compatible with the professional obligations of the lawyer."[150] Where

143. *Id.* cmt. 3 (including the use of "Internet-based service[s] to store client information").

144. *See id.*; *see also* MODEL RULES OF PROF'L CONDUCT R. 1.6(c).

145. *Security Overview*, *supra* note 110 ("Encryption for storage is applied after files are uploaded, and we manage the encryption keys.").

146. *Dropbox Privacy Policy*, *supra* note 134.

147. *Id.* ("We collect and store the files you upload . . . . If you add a file to your Dropbox that has been previously uploaded by you or another user, we may associate all or a portion of the previous file with your account rather than storing a duplicate.").

148. Soghoian, *supra* note 116 ("Encryption and deduplication are two technologies that generally don't mix well. If the encryption is done correctly, it should not be possible to detect what files a user has stored (or even if they have stored the same file as someone else), and so deduplication will not be possible.").

149. Hume, *supra* note 7, at 53 ("Consider the liability issue for uploading sensitive, proprietary client information to such a service.").

150. MODEL RULES OF PROF'L CONDUCT R. 5.3(a) (1983).

the end purposes are merely data storage and backup, the unfettered access to user data that Dropbox and its employees may exercise is contrary to the limitations in Model Rule 1.6. Allowing a third party full access to unencrypted data is not a reasonable effort, by either the attorney or the non-attorney assistant, to prevent the inadvertent or unauthorized disclosure of confidential client information.[151] The Model Rules consider the reasonableness of an attorney's efforts in determining if a breach of the duty of confidentiality has occurred.[152] The N.C. Rules, however, do not.[153] Rather than considering whether "reasonable efforts" have been made, North Carolina merely requires an attorney to "act competently to safeguard [confidential client information]."[154]

The remaining jurisdictions should adopt the August 2012 amendments to Rule 5.3 and its comments.[155] The adoption of the August 2012 amendments underscore the importance that an attorney make reasonable efforts to ensure that any non-attorney cloud service providers he uses are compatible with the attorney's own professional obligations, including the attorney's obligation to protect client information.[156] It is important to understand that neither the ABA Commission's amendments nor the existing N.C. Rules give room to rely on Dropbox's representation of safety and security in storing confidential client information due to Dropbox's unrestricted data access. Thus, the ILTSO recommends that only cloud vendors that are willing to observe standardized internal and external procedures should be employed.[157] If the procedures are included in a continuously updated and maintained uniform cloud user agreement, this may be the most effective method to protect an attorney and his clients from individual cloud user agreements.[158] The agreement may contain provisions mandating that

151. While this holds true for Dropbox, whose primary function is data backup and storage, it may not hold true for other cloud legal service providers that may involve document review and discovery, thereby necessitating access to unencrypted client files.

152. MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. 18.

153. *See generally* N.C. RULES OF PROF'L CONDUCT R. 1.6 (2003).

154. *Id.* cmt. 17.

155. *Variations of the ABA Model Rules of Professional Conduct: Rule 5.3 Responsibilities Regarding Nonlawyer Assistance*, *supra* note 58.

156. MODEL RULES OF PROF'L CONDUCT R. 5.3 cmt. 3.

157. ILTSO 2011 Guidelines, *supra* note 121, at 16.

158. The attorney who has opted into the realm of cloud computing likely has not done so to become an expert regarding the Internet and related security measures, but rather has done so to more efficiently manage his business and his clients' files. Providing the option for vetted cloud vendors or a compliant uniform agreement protects legal practitioners who lack experience in the complex, cloud computing world.

cloud service providers act in accordance with the professional obligations of attorneys, as required under Model Rule 5.3.

CONCLUSION

Cloud services are here to stay. Every draft of this Comment was auto-saved and synced on a personal Dropbox folder. Every e-mail that was sent regarding this Comment went through Gmail, a cloud-based consumer e-mail service. Most of the websites visited during preliminary research for this Comment were websites hosted in the cloud. Cloud services have become increasingly easy and useful for even the most ordinary user, to the extent that cloud technologies have become an integral (albeit at times invisible), part of our lives. For many, the appeal of universal accessibility and the low-cost, if any, of data storage and backup is too strong to ignore.

An attorney user of the cloud should be particularly watchful of the terms he agrees to because of the potential breach of his duty of confidentiality. An attorney must consider the convenience of Dropbox and similar cloud computing services and balance the rights of his clients and his own obligations as a licensed attorney. As a call to action, this Comment is meant to urge attorneys to consider the implications of their cloud usage and to likewise urge State Bars across the nation to at least consider the ABA Commission on Ethics 20/20 August 2012 amendments.

Eliu Mendez