Cloud Nine or Cloud Nein? Cloud Computing and Its Impact on Lawyers’ Ethical Obligations and Privileged Communications

Louise Lark Hill*

Law firms and lawyers are turning to “the cloud” as a convenient and cost effective alternative to traditional hard drive storage of material. “The cloud” is a metaphorical reference to a virtual platform where users interact with Internet applications and store data on shared distant servers. “Cloud computing” is the term employed when one stores or accesses information through these remote servers, which can be accomplished from anywhere there is Internet access, rather than from one’s hard drive storage. While using remote storage is both convenient and economical, with its use significant issues arise for lawyers. Among these issues are those relating to competence and confidentiality, and the effect that use of this mechanism may have on material that would otherwise be considered privileged.

This article will begin by addressing the phenomenon of the cloud and examine how cloud computing functions. Part II of the article will discuss a lawyer’s ethical obligation of competence and confidentiality, addressing whether these are compromised by turning information over to cloud service providers. Attorney-client privilege will be raised in Part III, along with an examination of the effect that out-source storage may have on otherwise privileged communications. Part IV will look to how jurisdictions have responded to questions raised about remote data storage and attempt to highlight common mandates of which lawyers should be aware.

Cloud Computing

In the early days of computer use, “the mainframe computing model allowed users to ‘operate on slices of a central server’s time and resources.’”¹ Companies either purchased their own mainframes, which were huge and had to be operated

* Distinguished Professor of Law, Widener University School of Law, Wilmington, Delaware.
by experts, or more typically, leased time on the mainframe of another company.\textsuperscript{2} As technology evolved, mainframe computing gave way to minicomputers,\textsuperscript{3} both of which were eclipsed by the personal computing model, which implemented software licensing and gave users physical control of their data.\textsuperscript{4} In the traditional software licensing model, a customer obtained an executable software code from a vendor and installed it on its own servers. Users who ran out of storage space, or needed more computer power, had to upgrade their software or hardware.\textsuperscript{5}

Now, in the second decade of the twenty-first century, it appears that the personal computing model is beginning to be eclipsed by the cloud. The concept of cloud computing “is a simple one—to harness the instantaneous remote access of the Internet and seemingly limitless storage for common use.”\textsuperscript{6} It is defined by The National Institute of Standards and Technology as “a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.”\textsuperscript{7} A user’s “data can be held in any location to which the cloud provider has access,” which “may be distributed across multiple machines in multiple countries.”\textsuperscript{8} Said to have revolutionized business practices, cloud computing allows “users of cloud services to off-load significant overhead and expenses for information technology (IT) functions while obtaining scalable and flexible computing services that do not depend on a specific location.”\textsuperscript{9}

\textsuperscript{3} Minicomputers were “‘mini’ only in reference to room-sized mainframe computers.” \textit{Id.} at 417. Minicomputers and mainframes “dominated the use of computers from the late 1940’s to the late 1970’s and even into the early 1980’s.” \textit{Id.} at 428.
\textsuperscript{4} \textit{Id.} at 423 & 428. “The invention of the microprocessor enabled the development of what we think of as the personal computer and thus brought the use of computing ability to ordinary people.” \textit{Id.} at 417.
\textsuperscript{5} See Kattan, \textit{supra} note 1, at 621-22.
\textsuperscript{7} Wayne Jansen & Timothy Grance, Guidelines on Security and Privacy in Public Cloud Computing, Draft Special Pub. 800-144, Nat’l Inst. of Standards and Tech. (Dep’t Commerce Jan. 2011) at 3 [hereinafter NIST Guidelines]. It has been noted that with respect to cloud computing, “there are many definitions and because cloud computing is evolving, those definitions tend to change and evolve as well.” James Mullan, \textit{Making Molehills out of Mountains: A Look at Some Emerging Technologies}, L.I.M. 2012, 12(1) 51-55, at 3.
\textsuperscript{9} \textit{Id.} at 48.
It “has accelerated the deconstruction of monolithic software systems into components of a ‘service-oriented architecture.’”

A familiar example of cloud application and storage are email accounts, such as those available from Hotmail or Gmail. Messages are received and stored on Hotmail or Gmail remote servers, which can be accessed by subscribers anywhere there is Internet access. “For a user, these cloud services achieve email functionality at no cost and with no requirement that the user have his own servers or any sort of technology infrastructure.” Cloud computing offers customers lower costs and “accommodates growth with dynamic access to resources and flexible purchasing plans . . . while maintaining instant and seemingly unlimited access to computing resources.”

Applying this concept to law practice, cloud computing allows lawyers a cost-effective and convenient way to store material and share this electronic data with others, such as clients or other lawyers. Apparently, the first law firms to take advantage of the cloud were the large ones, where the volume of data exceeded their in-house capabilities or where firms with multiple offices needed access to the same material. But the cloud is not limited to the large law firms. With things like pay-as-you-go plans, which “virtually guarantee significant cost savings,” very small law firms and solo practitioners have gotten “access to computing power and myriad application choices that were once the stuff of wish lists.” Since electronic storage can be obtained without a large capital investment, “[s]mall firms can provide services that larger firms have been providing for years, while limiting costs to an amount proportionate to their use.” In fact for these smaller law practice entities “the cost compression of cloud computing has made it the only financially viable model for managing electronically stored information.”

---

11. See Gladstone & Regan, supra note 6. Even though Google or Microsoft have possession and custody of the user’s Gmail or Hotmail account, typically these cloud service providers disclaim ownership of the user’s data, putting “control of the data in the hands of the clients.”
12. See Gladstone & Regan, supra note 6.
15. See Dysart, supra note 14, at 29.
17. See Dysart, supra note 14, at 29.
There are five characteristics of the cloud model, along with three service models and five deployment models.\textsuperscript{18} The five essential characteristics of cloud computing are on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service.\textsuperscript{19} With on-demand service, “[a] consumer can provision computing capabilities, such as server time and network storage, as needed automatically.”\textsuperscript{20} With broad network access, “[c]apabilities are network accessible by various client platforms.”\textsuperscript{21} With resource pooling, “[t]he provider’s computing capabilities are pooled to serve multiple consumers using a multi-tenant model. Resources are dynamically assigned and reassigned according to consumer demand.”\textsuperscript{22} With rapid elasticity, “[c]apabilities can be rapidly and elastically provisioned, in some cases automatically.”\textsuperscript{23} And with measured service, “[c]loud systems automatically control and optimize resource use by leveraging a metering capability.”\textsuperscript{24}

The three service models are Cloud Software as a Service [SaaS],\textsuperscript{25} Cloud Platform as a Service [PaaS]\textsuperscript{26} and Cloud Infrastructure as a Service [IaaS].\textsuperscript{27} SaaS is a model of software deployment where applications and computational resources to run the applications “are provided for use on demand as a turnkey service.”\textsuperscript{28} With SaaS, which is delivered through a password-protected website, typically “the user does not know where the data is being held, who is managing the servers holding the data, or how the data is being delivered.”\textsuperscript{29} PaaS is a model of software deployment where “the computing platform is provided as an on-demand service upon which applications can be developed and deployed.”\textsuperscript{30}


\textsuperscript{19} Id.

\textsuperscript{20} Id.

\textsuperscript{21} Id. Examples of these would be mobile phones, laptops, and PDAs. Id.

\textsuperscript{22} Id. Typically the customer has no control or knowledge of exactly where the provided resource is located. Id. This is the case even though “you send a client’s information over the Internet to real servers in real locations.” John Jocelyn, \textit{Don’t Have Your Head in the Cloud, Know Your Cloud-Computing Related Duties to Clients}, 54 DRI FOR DEP. 4, at 76 (April 2012).

\textsuperscript{23} Bowen, supra note 18, at 1. The available capabilities for provisioning “can be purchased in any quantity at anytime.” Id.

\textsuperscript{24} Id.

\textsuperscript{25} The capability provided with SaaS is use of the provider’s applications. These run on a cloud infrastructure and are accessible through a Web browser. Id.

\textsuperscript{26} The capability provided with PaaS is deployment of consumer-created or acquired applications onto the cloud infrastructure, which use programming languages and tools supported by the provider. Id.

\textsuperscript{27} The capability provided with IaaS is the provision of fundamental computing resources (e.g., processing, storage, networks) where the consumer can deploy and run arbitrary software, including operating systems and applications. Id.

\textsuperscript{28} NIST Guidelines, supra note 7, at 3.

\textsuperscript{29} Hinkes & Gaukroger, supra note 8, at 49.

\textsuperscript{30} NIST Guidelines, supra note 7, at 4.
PaaS allows a user to launch an application using infrastructure components that are supported by the provider,31 and security provisions are usually split between the user and the cloud provider.32 IaaS is a model of software deployment where basic computing infrastructure is provided as a service which is on-demand, “upon which a platform to develop and execute applications can be established.”33 With IaaS, the server space, computing processor cycles, and hardware/software maintenance are outsourced to a third party and typically, “the user has no access to or responsibility for the maintenance of the infrastructure.”34 It is the SaaS service model that is typically sold to law firms.35 Tools for practice and document management, payroll, human resources, tax systems and filtering are among the SaaS applications law firms use.36

Added to the three service models for cloud computing are the four models for deploying cloud services. These are the private cloud, which is operated solely for an organization; the community cloud, where the cloud infrastructure is shared by several organizations; the public cloud, where the cloud infrastructure is made available to the public or to a large group; and the hybrid cloud, which is composed of two or more of the preceding clouds, and are unique entities but are bound together to permit data and application portability.37 Just as service models differ, so does the model for deploying cloud services. Lawyers making use of cloud computing must be aware of the characteristics of cloud computing and understand that selection of “[t]he appropriate model depends on the nature of the services as well as the potential sensitivity of the systems being implemented or data being released into the cloud.”38

Because of the components associated with cloud computing, data held in the cloud differs from a traditional third-party vendor who houses an organization’s material. The traditional third-party vendor typically stores “only data produced by local users on local machines, data that are primarily held on local servers, from which the data are transmitted to remote vendor systems.”39 With cloud computing, a user’s “data can be held in any location to which the cloud provider has access; data may be distributed across multiple machines in multiple countries and may be highly dynamic.”40 These characteristics relating to resource pooling, which contribute to the ethical questions lawyers face, are

31. See Bowen, supra note 18, at 1.
32. See NIST Guidelines, supra note 7, at 4. Arguably, this component fosters innovation. See Grunwald, supra note 10, at 429.
33. NIST Guidelines, supra note 7, at 4.
34. See Hinkes & Gaukroger, supra note 8, at 49.
35. See Mullan, supra note 7, at 3.
36. Id.
37. See Bowen, supra note 18, at 1-2. See also infra note 138.
38. Bowen, supra note 18, at 2.
39. Hinkes & Gaukroger, supra note 8, at 49.
40. Id.
what help to make the cloud cost effective and convenient, and therefore spur its popularity.\footnote{The movement of data among available data center resources maximizes the efficiencies of the system and is “a reasonably good solution to the problem of under-used machines.” Bowen, \textit{supra} note 18, at 5.}

**Ethical Obligations**

The ethical obligations associated with a lawyer’s use of cloud computing are wide ranging. Traditionally, “client property was handled and stored on site (or in an off site storage facility) and lawyer-client communications occurred in person.”\footnote{Vt. B. Ass’n Advisory Op. 2010-6 (2011).} With technological advances, however, there have been changes “in the way data is transmitted and stored, and the way lawyers communicate with clients.”\footnote{Id.} A prime example of this is the use of electronic communications, which have become “an integral part of legal practice.”\footnote{Louise L. Hill, \textit{Emerging Technology and Client Confidentiality: How Changing Technology Brings Ethical Dilemmas}, 16 B.U. J. SCI. & TECH. L. I, 20 (2010).} Typically, a cloud service provider does not intend to share the content of stored documents with a user, but “is merely providing a platform for using and storing the content via the cloud.”\footnote{David A. Couillard, \textit{Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing}, 93 ONLINE SEARCH & SEIZURE 2205, 2237 (2009).} However, not surprisingly, the advent of the lawyer’s use of cloud computing is accompanied by significant issues relating to a lawyer’s ethical obligations, and in particular those that relate to the privacy and security of client information.

Cloud computing notwithstanding, lawyers are obligated to competently represent clients, maintain client confidences, safeguard client property and make sure those with whom they work do the same. The American Bar Association Model Rules of Professional Conduct, on which the individual states base their rules that govern lawyer conduct,\footnote{Hill, \textit{supra} note 44, at 15. While the individual states follow the Model Rule format, lawyers are not provided with a uniform standard since “[i]nterpretational differences exist among the jurisdictions, as do differences in the text of some of the rules.” \textit{Id.} at 15 n.97.} address competence in its first substantive rule. Model Rule 1.1 states “[a] lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.”\footnote{MODEL RULES OF PROF’L CONDUCT R. 1.1 (2012).} The matter of confidentiality of information is addressed at Model Rule 1.6, stating in part, “[a] lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent . . . .”\footnote{\textit{Id.} at R 1.6(a). Prior to being amended in August, 2012, comments 16 and 17 to Rule 1.6, addressing acting competently to preserve information, provided as follows:}
calls for client property to be held “separate from the lawyer’s own property . . . be identified as such and appropriately safeguarded.”\(^{49}\) And Model Rule 5.3 requires lawyers with managerial or supervisory authority over nonlawyers to see that “the person’s conduct is compatible with the professional obligations of the lawyer.”\(^{50}\)

When a lawyer turns client information over to a cloud service provider, Model Rules 1.1, 1.6, 1.15 and 5.3 are among the rules implicated. To maintain client confidences and safeguard client property, a lawyer’s duty of competence requires the lawyer to protect client information that is directly accessible or gleaned from the cloud systems. In that there are many contracting models under which cloud services are offered,\(^{51}\) the competent lawyer must select the appropriate model, which necessitates understanding the risks inherent in the use of cloud computing. It was noted nearly a decade ago that with respect to transmitting electronic documents, “reasonable care may call for the lawyer to stay abreast of technological advances and potential risks . . .”\(^{52}\) More recently, “understanding relevant technology’s benefits and risks” has been recognized as a requirement of lawyer competence.\(^{53}\) Clearly this is something called for when engaging in cloud services.

After nearly three years of work, in May of 2012, the American Bar Association [ABA] Commission on Ethics 20/20 [Ethics 20/20] presented proposals

\[\text{Id. at R. 1.6 cmts. 16 & 17 (2011).}\]
\[\text{49. Id. at R. 1.15(a)(1) (2012).}\]
\[\text{50. Id. at R. 5.3(a) & (b). Model Rule 5.3(a) calls for lawyers with managerial authority in a law firm “to ensure that the firm has in effect measures giving reasonable assurance that the person’s conduct is compatible with the professional obligations of the lawyer.” Model Rule 5.3(b) calls for lawyers having direct supervisory authority over a nonlawyer to “make reasonable efforts to ensure that the person’s conduct is compatible with the professional obligations of the lawyer.” Id.}\]
\[\text{51. See Bowen, supra note 18, at 2.}\]
\[\text{52. Hill, supra note 44, at 25 (quoting N.Y. State Bar Ass’n Op.782 (Dec. 8, 2004)).}\]
for updating the Model Rules “to keep pace with social change and the evolution of law practice.” Created by the ABA in 2009 “to tackle the ethical and regulatory challenges and opportunities arising from these 21st century realities,” Ethics 20/20 specifically addressed technology in its 2012 recommendations since it “affects nearly every aspect of legal work.” Part of the technology examination in which Ethics 20/20 engaged related to technology and confidentiality, because “technology has transformed how lawyers communicate with their clients and store their client confidences.” The transformation from “attorney-client communications by telephone, in person, fax and letter to electronic communication and storage of those communications on law firm and third-party servers, mobile devices, flash drives, etc. have raised new concerns about data security and lawyers’ ethical obligations to protect client confidences.” To this end, Ethics 20/20 suggested changes to Model Rules 1.1, 1.6 and 5.3. These recommendations, along with changes to a number of other Model Rules, were approved and adopted by the ABA House of Delegates at their Annual Meeting on August 6, 2012.

Ethics 20/20 recommended, and the ABA approved, that a comment be added to Model Rule 1.1, which addresses Competence, “to make explicit that a lawyer’s duty of competence, which requires the lawyer to stay abreast of changes in the law and its practice, includes understanding relevant technology’s benefits and risks.” Specifically, comment 8 (previously comment 6) of Model Rule 1.1 was amended to provide as follows: “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.”62 It was felt the inclusion of this language offers “greater clarity regarding this duty and emphasize[s] the growing importance of technology to modern law practice.”63

Model Rule 1.6, which addresses Confidentiality of Information, also has changes to both the rule itself and its commentary. The purpose of these changes was to “make clear that a lawyer has an ethical duty to take reasonable measures to protect a client’s confidential information from inadvertent disclosure, unauthorized disclosure, and unauthorized access, regardless of the medium used.”64 Although this obligation was referenced in former commentary to Rule 1.6,65 the Ethics 20/20 Commission “concluded that technological change has so enhanced the importance of this duty that it should be identified in the black letter of Rule 1.6 and described in more detail through additional Comment language.”66 A new paragraph (c) was added to Model Rule 1.6, stating as follows: “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.”67 In concert with the rule addition, Comment 16 of Model Rule 1.6 now reads:

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 or entities who are participating in the representation of the client or who are subject to the lawyer’s supervision. See Rules 1.1, 5.1 and 5.3. The unauthorized access to, or the inadvertent or unauthorized disclosure of, confidential information does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure. Factors to

63. Ethics 20/20 Intro., supra note 53, at 8.
64. Id.
65. See supra note 48.
67. MODEL RULES OF PROF’L CONDUCT R. 1.6(c) (2012). In another set of recommendations, Ethics 20/20 suggested that an additional exception be added to Model Rule 1.6(b) that would permit disclosure of client information to identify and resolve conflicts of interest when lawyers are considering changing firms, merging firms or selling a law practice. See Law. Manual on Prof’l Conduct, supra note 54, at 310. It was suggested, and approved by the ABA, that (b)(7) be added to Model Rule 1.6, allowing a lawyer to reveal information relating to the representation of a client to the extent the lawyer reasonably believes necessary “to detect and resolve conflicts of interest between lawyers in different firms, but only if the relevant information would not compromise the attorney-client privilege or otherwise prejudice the client.” MODEL RULES OF PROF’L CONDUCT R. 1.6(b)(7) (2012). Also suggested, and approved, was the addition of two comments that would explain the rule and impose limitations to help protect clients. A.B.A. Comm’n on Ethics 20/20 Rep. on Resolution of Cmts to Model Rule 1.6 (Confidentiality) (Aug. 2012); Law. Manual on Prof’l Conduct, supra note 60, at 509.
be considered in determining the reasonableness of the lawyer’s efforts include, but are not limited to, 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 (e.g., by making a device or important piece of software excessively difficult to use). A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule. Whether a lawyer may be required to take additional steps to safeguard a client’s information in order to comply with other law, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules. For a lawyer’s duties when sharing information with nonlawyers outside the lawyer’s own firm, see Rule 5.3, Comments [3]-[4].

Comment 17 to Model Rule 1.6 was also amended by adding a sentence to the end of the existing comment. The following now concludes Comment 17: “Whether a lawyer may be required to take additional steps in order to comply with other law, such as state and federal laws that govern data privacy, is beyond the scope of these Rules.” With the Model Rule 1.6 changes, Ethics 20/20 recognized that lawyers “cannot guarantee electronic security” and noted that

68. MODEL RULES OF PROF’L CONDUCT R. 1.6 cmt. 16 (2012).
69. Id. at R. 1.6 cmt. 17. Almost all states within the United States require that when there is a data breach, affected persons be notified. See Bowen, supra note 18, at 2. With respect to data breach law, “data in the cloud is treated no differently from any other electronically stored information.” Id. In addition to laws directed at data breach, many states also have data security requirements calling for entities to obtain “contractual guarantees that technology vendors (including cloud providers) will provide adequate security.” Id. at 4. On the federal level, the Gramm-Leach-Bliley Act [GLB] requires financial institutions to have procedures which protect against unauthorized access to information and ensure confidentiality of personal information. Id. at 2. The Safeguards Rule, called for in GLB and enforced by the Federal Trade Commission [FTC], requires financial services providers to have written security plans to protect customer information. The Red Flag Rules, promulgated by the FTC in 2007 as part of the Fair and Accurate Credit Transactions Act of 2003 (The Red Flag Program Clarification Act was enacted December 22, 2010), call for financial institutions and credit account holders to have written identity theft programs. Id. at 3. The Red Flag Rules apply to cloud providers that are creditors, just as they would to any other company operating in an off-line physical space. Id. The Electronic Communications Privacy Act [ECPA] provides protection to many electronic communications, which would encompass most data held by cloud providers. Id. at 3-4. However, the ECPA has provisions which may require a cloud provider to disclose data it holds to the federal government, as would certain provisions in the USA Patriot Act. Id. It has been noted that “(a) cloud provider may find itself in the awkward position of being required to provide information on a cloud user or a cloud user’s customer to the U.S. government without providing notice to the cloud user.” Id. at 3.
imposing a duty on lawyers “to achieve the unattainable” is not intended.\textsuperscript{70} Rather the changes identify factors for a lawyer to consider when determining whether precautions are reasonable.\textsuperscript{71} For instance, as noted in new Comment 16, things such as the cost of safeguards, their difficulty of implementation, and the sensitivity of information are among the things to be considered to this end.

Model Rule 5.3, which addresses Responsibilities Regarding Nonlawyer Assistance, has also been changed. The outsourcing of legal and nonlegal services is the primary target of the Model Rule 5.3 amendments.\textsuperscript{72} The term “outsourcing” refers to “taking a specific task or function previously performed within a firm or entity and, for reasons including cost and efficiency, having it performed by an outside service provider, either in the United States or another country.”\textsuperscript{73} To this end, matters related to cloud computing are specifically implicated within the 2012 alterations.\textsuperscript{74} While Ethics 20/20 did not suggest any changes to the language of the rule itself, a change in the title of the rule was put forward, substituting the term “Assistance” for “Assistants,” and changes in the commentary of the rule were proposed.\textsuperscript{75}

It is the design of Model Rule 5.3 to make sure that lawyers appropriately supervise the nonlawyers with whom they work.\textsuperscript{76} To provide additional guidance on the application of the rule, Ethics 20/20 suggested, and the ABA approved, an addition to the commentary of Model Rule 5.3 that specifically addresses “Nonlawyers Outside the Firm.” A new Comment 3 provides as follows:

A lawyer may use nonlawyers outside the firm to assist the lawyer in rendering legal services to the client. Examples include the retention of an investigative or paraprofessional service, hiring a document management company to create and maintain a database for complex litigation, sending client documents to a third party for printing or scanning, and using an Internet-based service to store client information. When using such services outside the firm, a lawyer must make reasonable

\textsuperscript{70} Ethics 20/20 Intro., supra note 53, at 8.
\textsuperscript{71} Id.
\textsuperscript{72} See Id. at 12; Law. Manual on Prof’l Conduct, supra note 54, at 309. Although outsourcing is targeted in the Model Rule 5.3 changes, the term “outsourcing” is not used in the proposed commentary because “lawyers may incorrectly conclude that they are not engaged in ‘outsourcing’ when using nonlawyer services outside the firm.” A.B.A. Comm’n on Ethics 20/20 Rep. on R. 5.3, at 8 (Aug. 2012).
\textsuperscript{73} Id. at 2. When giving examples of law-related work that is frequently outsourced, the Report notes “investigative services, offsite online data storage or online practice management tools (e.g., “cloud computing” services), and creation and maintenance of databases to manage discovery in litigation.” Id. at 2-3. The Report goes on to state that “[o]utsourcing also occurs when lawyers retain other lawyers and law firms to conduct a range of services, such as legal research, document review, patent searches, due diligence, and contract drafting.” Id. at 3.
\textsuperscript{74} See infra note 77 and accompanying text.
\textsuperscript{76} A.B.A. Comm’n on Ethics 20/20 Rep. on R. 5.3, supra note 72, at 6.
efforts to ensure that the services are provided in a manner that is compatible with the lawyer’s professional obligations. The extent of this obligation will depend upon the circumstances, 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 jurisdiction in which the services will be performed, particularly with regard to confidentiality. . .When retaining or directing a nonlawyer outside the firm, a lawyer should communicate directions appropriate under the circumstances or give reasonable assurance that the nonlawyer’s conduct is compatible with the professional obligations of the lawyer.77

An interest of the Commission was the protection of confidential information, and in particular, the procedures used to accomplish that end.78 In that “using an Internet-based service to store client information” is specifically referenced as an example of using the assistance of nonlawyers, new Comment 3 emphasizes that reasonable efforts must be used to make sure client information is safeguarded and remains confidential when employing the mechanisms of the cloud. Apparently, mindful of the variations in the scope and application of confidentiality law from jurisdiction to jurisdiction, “the legal and ethical environments of the jurisdiction in which the services will be performed” is noted as a circumstance to be considered in fulfilling the obligations of the lawyer.

While changes were suggested, and approved, for Model Rule 1.1, 1.6 and 5.3, no changes were suggested to Model Rule 1.15. Considering the fact that the lawyer’s role is shaped by forces other than the Model Rules, such as by court rules, statutes and ethics opinions, the Commission felt in some instances there were Rules where no special language needed to be added to remind lawyers how they would be applicable to outsourcing practices.79 The Commission felt that Model Rule 1.15, on Safekeeping Property, was one of these rules.80 However, to help lawyers understand their obligations to protect client information in this digital environment, Ethics 20/20 also proposed that the ABA create and maintain a website that would provide lawyers with specific and timely guidance on technology that lawyers commonly encounter.81

Attorney-Client Privilege

In addition to a lawyer’s ethical duty to maintain client confidences, the law of confidentiality in the United States recognizes the doctrine of attorney-client

77. A.B.A. Comm’n on Ethics 20/20 Resolution on R. 5.3, supra note 75, cmt. 3.
79. Id. at 4.
80. Id. at 5. See supra note 49 and accompanying text.
privilege, which is related to, but distinct from, the lawyer’s ethical duty.\textsuperscript{82} Attorney-client privilege essentially protects against compelled disclosure of confidential communications exchanged between lawyer and client.\textsuperscript{83} It is a rule of evidence, applicable in civil and criminal proceedings, limiting “the extent to which a party in litigation can force from an unwitting witness a statement or document that is protected as confidential.”\textsuperscript{84} A lawyer’s ethical duty to maintain client confidences, on the other hand, is “not limited to judicial or other proceedings, but rather appl[ies] in all representational contexts.”\textsuperscript{85}

The Restatement (Third) of the Law Governing Lawyers defines attorney-client privilege as: (1) a communication; (2) made between privileged persons; (3) in confidence; (4) for the purpose of obtaining or providing legal assistance to the client.\textsuperscript{86} Each state in the United States has its own privilege rules, which generally follow the common law, while Rule 501 of the Federal Rules of Evidence governs federal courts.\textsuperscript{87} Outside of the United States, “the scope and application of legal professional privilege varies widely from country to country.”\textsuperscript{88} Within the civil law systems, codes of procedure or codes of practice often include provisions precluding lawyers from disclosing confidential commu-


\textsuperscript{84} Wolfram, supra note 82, at 541-42.

\textsuperscript{85} Arthur Garwin, Confidentiality and Its Relationship to the Attorney-Client Privilege, in ATTORNEY-CLIENT PRIVILEGE IN CIVIL LITIGATION 161, 162 (Vincent S. Walkowiak, Stephen M. McNabb, Oscar Rey Rodriguez eds., 2012).

\textsuperscript{86} RESTATEMENT (THIRD) OF THE LAW GOVERNING LAWYERS sec. 68 (2000).

\textsuperscript{87} See Daiske Yoshida, The Applicability of the Attorney Client Privilege to Communications with Foreign Legal Professionals, 66 FORDHAM L. REV. 209, 213 (1997). The Federal Rules of Evidence provide:

\textit{FED. R. EVID. 501.}

communications between the lawyer and client.\textsuperscript{89} “It is not that the communication itself is privileged, but that the lawyer is under a duty not to disclose the information in it.”\textsuperscript{90}

Attorney-client privilege can be waived; and waiver of the privilege is absolute, being “construed broadly against the party claiming the privilege.”\textsuperscript{91} Waiver can result from intentional voluntary disclosure as well as from inadvertent disclosure.\textsuperscript{92} At issue is whether waiver is triggered when confidential information is turned over to a cloud service provider. In such a situation, not only is a lawyer entrusting protected information to a third party, but also, in the cloud environment, it is possible for the same information to be stored in multiple locations at the same time.\textsuperscript{93} Due to the fact that data may be moved geographically to servers in different states or different countries, a matter that is inherent in cloud service offerings, which jurisdiction or country’s laws are applicable may impact the privileged nature of underlying communications.\textsuperscript{94}

With respect to voluntary waiver, “[t]he client, not counsel, can voluntarily waive the privilege.”\textsuperscript{95} If a client voluntarily discloses privileged communications to non-privileged persons, “a court will feel free to find that, in this instance, the assurance of confidentiality was not important to the client, and that the general policy of free access by adversaries to all relevant evidence should prevail.”\textsuperscript{96} Opinion differs, however, on whether attorney-client privilege is waived with inadvertent disclosure.\textsuperscript{97} Most courts weigh circumstances that surround an inadvertent disclosure when determining if the privilege should continue to attach.\textsuperscript{98} Known as “the balancing test,” when considering if privilege has been waived, courts generally consider the reasonableness of precautions taken to prevent disclosure, the time taken to recognize the error, the scope of the production, the extent of the disclosure, and considerations of fairness and justice.\textsuperscript{99} Amend-

\begin{itemize}
\item \textsuperscript{90} \textit{Id}.
\item \textsuperscript{91} Mackintosh & Angus, \textit{supra} note 82, at 43.
\item \textsuperscript{92} \textit{Id}. Waiver can also result from the offensive use of otherwise privileged communications. The offensive use doctrine is triggered when a party to a proceeding introduces an issue related to advice received from a lawyer, impliedly waiving the confidentiality of the communication. \textit{Id}. at 43 n.57 (citing Chevron Corp. v. Pennzoil Co., 974 F.2d 1156, 1162 (9th Cir.1992)).
\item \textsuperscript{93} See Bowen, \textit{supra} note 18, at 5.
\item \textsuperscript{94} \textit{Id}. at 2.
\item \textsuperscript{95} Mackintosh & Angus, \textit{supra} note 82, at 42-43.
\item \textsuperscript{96} Wolfram, \textit{supra} note 82, at 544.
\item \textsuperscript{97} See Hill, \textit{supra} note 44, at 7.
\item \textsuperscript{98} \textit{Id}. at 8.
\item \textsuperscript{99} See Mackintosh & Angus, \textit{supra} note 82, at 45 n.87. Along with the balancing test, other recognized tests are “the strict responsibility test” and “the subjective intent test.” With the strict responsibility test, disclosure waives attorney-client privilege, even inadvertent disclosure. It is the traditional test, which puts the “risk of insufficient precautions [ ] on the client.” 8 \textsc{John Henry Wigmore et al., Evidence in Trials at Common Law} sec. 2325(3), at 633 (4th ed., rev.
ments to the Federal Rules of Evidence in 2008 addressed attorney-client privilege and inadvertent disclosure in federal court litigation.\textsuperscript{100} Rule 502(b) of the Federal Rules of Evidence was amended to provide that disclosure of privileged material does not result in the waiver of attorney-client privilege, provided: 

“(1) the disclosure is inadvertent; (2) the [party responsible for the disclosure] took reasonable steps to prevent disclosure; and (3) the [party responsible for the disclosure] took reasonable steps to rectify the error” after it occurred.\textsuperscript{101}

From the standpoint of privilege, at issue is whether turning confidential information over to a cloud service provider results in the waiver of attorney-client privilege. It stands to reason that in understanding and protecting against risks associated with cloud computing, a lawyer must assess the degree of protection needed to safeguard client information and act accordingly. This relates to competence as well as to the lawyer’s obligation to maintain client confidences and protect privileged communications. Entrusting confidential information to a cloud service provider without knowing what security methods are employed to protect electronic information, or where the information will be stored, may breach a lawyer’s ethical obligations and additionally, constitute inadvertent waiver, which would cause confidential information to lose its privileged status.

Noted in the Ethics 20/20 Commission’s Report is the fact that many outsourcing providers use security measures to protect electronic information, including things such as encryption, malware protection and firewalls, as well as measures to ensure that physical access to the electronic data is only by authorized employees.\textsuperscript{102} Additionally, the Report notes that many outsourcing providers require their lawyer and nonlawyer employees to sign confidentiality agreements.\textsuperscript{103} Lawyers must be aware of what safeguards a cloud service provider employs. In addition to data security issues, a lawyer must know what will happen to the data if the cloud provider is acquired, files for bankruptcy, or goes out of business.\textsuperscript{104} Failing to do so may have ethical implications and result in communications losing their privileged status through inadvertent waiver.


\textsuperscript{101} Fed. R. Evid. 502(b).

\textsuperscript{102} A.B.A. Comm’n on Ethics 20/20 Rep. on R. 5.3, \textit{supra} note 72, at 3-4. Among the security provisions noted are video monitoring, monitoring of employee computers, repeated identity checks, background checks on employees and periodic audits of the security measures. Outsourcing providers also “frequently disable the portals on employee computers so that portable data storage devices cannot be used to remove information from the premises.” \textit{Id.} at 4.

\textsuperscript{103} \textit{Id.} at 3.

\textsuperscript{104} See Bowen, \textit{supra} note 18, at 3.
Lawyers must be particularly sensitive to where data is stored when it is released into the cloud, since this may impact what country’s law would govern in a particular setting. In civil law countries, while “lawyer confidentiality obligations are complementary with privilege against compelled disclosure, the two are ‘conceptually different nonetheless and therefore mutually independent.’”105 For instance, in some countries only documents in the possession of the lawyer are protected.106 “Other documents, even a letter of legal advice from a lawyer, may not be protected in the client’s hands.”107 Also, in many countries the legal profession is bifurcated and, unlike in the United States, the attorney-client privilege as we know it does not extend to in-house lawyers.108 Therefore, documents stored in the cloud by in-house counsel that would be considered confidential and subject to privilege in the United States, may not have that status in other countries. Should the laws of these jurisdictions be triggered with respect to remote service providers located within their boundaries, the privileged nature of a communication could be compromised. For data in these “data centers may be subject to foreign laws or no laws at all.”109

Positions Taken by Jurisdictions

Due to the fact that an increasing number of lawyers and law firms have turned to the cloud for business functions, including document storage, bar associations and individual jurisdictions have addressed a number of ethical issues associated with cloud computing. Apparently mindful of the fact that remote document storage is here to stay, the tendency of these varied opinions is to allow the use of cloud computing, but qualify this approval with explicit safeguards. Not surprisingly, a primary concern of those who have reviewed the matter focuses on preserving the security and confidentiality of any stored material.


106. See Good, supra note 89. While there are exceptions, such as in criminal proceedings, privilege does not extend to material in the client’s possession in Switzerland and Germany. Id. 107. Hill, supra note 88, at A-129 (citing Good, supra note 89).

108. Id. at A-128. It is noted that:

[a] bias against international in-house counsel springs from doubt as to the professional independence of this category of practitioner. In some countries, the ‘independence that is called for in legal practice is evidenced by self-employment. ‘[R]easoning that financial reliance on a single employer must necessarily entail the surrender of ethical autonomy,’ in certain jurisdictions lawyers serving as in-house counsel must resign bar membership, if they are admitted, or be placed on inactive status during the time they are employed.

Id. (quoting Mary C. Daly, The Cultural, Ethical, and Legal Challenges in Lawyering for a Global Organization: The Role of General Counsel, 46 EMORY L.J. 1057, 1102 (1997)).

Alabama

In Alabama, the General Counsel, with the concurrence of the Disciplinary Commission of the Alabama State Bar, determined that “a lawyer may use ‘cloud computing’ or third-party providers to store client data provided that the attorney exercises reasonable care in doing so.”110 Encompassed in this duty of reasonable care is the requirement that lawyers become knowledgeable about how the data will be stored and its security, and “to reasonably ensure that the provider will abide by a confidentiality agreement in handling the data. Additionally, because technology is constantly evolving, the lawyer will have a continuing duty to stay abreast of appropriate security safeguards that should be employed by the lawyer and third-party provider.”111

Arizona

The Committee on Rules of Professional Conduct of the State Bar of Arizona determined that “lawyers providing an online file storage and retrieval system for client access of documents must take reasonable precautions to protect the security and confidentiality of client documents and information.”112 The committee noted it is “important that lawyers recognize their own competence limitations regarding computer security measures and take the necessary time and energy to become competent or alternatively consult available experts in the field.”113 Also the committee cautioned that any selected security measures should be periodically reviewed, since “technology advances may make certain protective measures obsolete over time.”114

California

The Standing Committee on Professional Responsibility and Conduct of the State Bar of California determined that “[w]hether an attorney violates his or her duties of confidentiality and competence when using technology to transmit or store confidential client information will depend on the particular technology being used and the circumstances surrounding its use.”115 Among the things to be considered by lawyers before using a given technology are the technology’s level of security, the information’s sensitivity, the urgency of the matter, the possible effect inadvertent disclosure or unauthorized interception could pose to a client or third party, as well as client instructions and circumstances.116

111. Id.
113. Id.
114. Id.
116. Id.
Iowa

Recognizing that the protection called for with client information varies depending on the client, matter and information involved, the Committee on Ethics and Practice Guidelines of the Iowa State Bar Association has indicated that SaaS may be used by lawyers, “[b]ut it places on the lawyer the obligation to perform due diligence to assess the degree of protection that will be needed and act accordingly.”117 Noting that “due diligence must be performed by individuals who possess both the requisite technology expertise and as well as an understanding of the Iowa Rules of Professional Conduct,” the Committee suggests that specific inquiries be made relating to data accessibility and protection that will be afforded the stored material.118

Maine

The Professional Ethics Commission of the Maine Board of Overseers of the Bar has determined that with appropriate safeguards, a lawyer may use a remote computer server backup service to store confidential electronic data without violating the lawyer’s ethical obligation to maintain client confidentiality.119 Mindful of “the pervasive and changing use of evolving technology,” the Commission declined to state particular safeguards to be employed by lawyers, but rather outlined “guidance for lawyers to consider in determining when professional obligations are satisfied.”120 To that end, the Commission stated that at a minimum, steps should be taken to make sure that the company providing storage has a legally enforceable obligation to maintain the confidentiality of the client data it stores.121

Nevada

The Standing Committee on Ethics and Professional Responsibility of the State Bar of Nevada has determined that a lawyer may store confidential client information or communications on a server that is outside the lawyer’s direct supervision and control, provided the lawyer acts “competently and reasonably to safeguard the material from inadvertent and unauthorized disclosure.”122 Comparing this situation to the storage of paper documents containing confidential client information in a third party warehouse, the committee stated that “[w]hile a lawyer is not strictly liable for any breach of client confidentiality, his duty includes reasonable precautions to prevent both accidental and unauthorized disclosure.”123

118. Id.
120. Id.
121. Id.
123. Id.
New Jersey

The Advisory Committee on Professional Ethics, appointed by the New Jersey Supreme Court, when responding to an inquiry relating to an electronic filing system and e-mailing documents, noted “[i]t is very possible that a firm might seek to store client sensitive data on a . . . web server provided by an outside Internet Service Provider (and shared with other clients of the ISP) in order to make such information available to clients, where access to that server may not be exclusively controlled by the firm’s own personnel.” 124 Reluctant to impose requirements tied to “a specific understanding of technology that may very well be obsolete tomorrow,” the Committee called for reasonable care to be taken against unauthorized disclosure. 125 To this end, the Committee stated the party to whom such material is entrusted must have an enforceable obligation to preserve confidentiality and security, and use must be made of available technology “to guard against reasonably foreseeable attempts to infiltrate the data.” 126

New York

The Committee on Professional Ethics of the New York State Bar Association has determined that a lawyer may use cloud computing provided by an online service to backup file storage, provided “the lawyer takes reasonable care to ensure that the system is secure and that client confidentiality will be maintained.” 127 The Committee noted that reasonable care to protect against unauthorized disclosure may include the following steps:

• ensuring that the provider has enforceable obligations to preserve confidentiality and security, and that the provider will notify the lawyer if served with process calling for production of client information;
• investigating the provider’s procedures, such as those relating to security and recoverability, to determine their adequacy;

125. Id. When inferring the use of what has become known as cloud computing, and a lawyer’s obligation to maintain client confidences, the Commission said it would not impose: a per se requirement that, where data is available on a secure web server, the server must be subject to the exclusive command and control of the firm through its own employees, a rule that would categorically forbid use of an outside ISP. The very nature of the Internet makes the location of the physical equipment somewhat irrelevant, since it can be accessed remotely from any other Internet address. Such a requirement would work to the disadvantage of smaller firms for which such a dedicated IT staff is not practical, and deprive them and their clients of the potential advantages in enhanced communication as a result.
employing available technology to guard against infiltration of the stored data."128

The Committee cautioned that lawyers “should periodically reconfirm that the provider’s security measures remain effective in light of advances in technology,” as well as monitor changes in the law relating to confidential communication, “especially regarding instances when using technology may waive an otherwise applicable privilege.”129

North Carolina

The Ethics Committee of the North Carolina State Bar has approved the use of SaaS by a law firm, “provided steps are taken to minimize the risk of inadvertent or unauthorized disclosure of confidential client information and to protect client property, including the information in a client’s file, from risk of loss.”130 To this end, the Committee does not set forth specific security requirements, but calls for “due diligence and frequent and regular education”131

The Committee did posit some recommended security measures, however, including:

• an agreement on how the vendor will handle confidential client information in keeping with the lawyer’s professional responsibilities;
• a method for the lawyer to retrieve data should there be a break in service continuity;
• careful review of an agreement’s terms, including security policies;
• evaluation of measures for safeguarding the security and confidentiality of stored data;
• evaluation of the extent to which the provider backs up hosted data.132

Pennsylvania

The Committee on Legal Ethics and Professional Responsibility of the Pennsylvania Bar Association determined that a lawyer may store confidential client information using cloud computing, provided “the lawyer takes reasonable care to assure that (1) all such materials remain confidential, and (2) reasonable safeguards are employed to ensure that the data is protected from breaches, data loss and other risks.”133 While noting that “measures necessary to protect confidential information will vary based upon the technology and infrastructure of each

128. Id.
129. Id.
131. Id.
132. Id.
office,” the Committee stated that “there are common procedures and safeguards that attorneys must employ” With cloud computing, the standard of reasonable care may include the following:

- backing up data
- installing firewalls
- limiting information available to unauthorized persons
- avoiding inadvertent disclosure of information
- encrypting confidential data
- implementing monitoring procedures
- creating plans to address security breaches
- investigating and ensuring the provider has adequate safeguards, security and reliability to meet the ethical obligations of the lawyer

Mindful that a server used by a provider may be kept in a country other than the United States, the Committee states “an attorney must ensure that the data in the server is protected by privacy laws that reasonably mirror those of the United States.” Also, the Committee asserts that “[l]awyers may need to consider that at least some data may be too important to risk inclusion in cloud services.” And with an eye toward security against data breaches, the Committee offered the use of private or hybrid clouds as alternatives to community or public clouds.

---

134. Id.
135. Id. According to the Committee, the lawyer should ensure that the provider does the following:
   - explicitly agrees it has no ownership or security interest in the data;
   - has an enforceable obligation to preserve security;
   - will notify the lawyer if requested to produce data to a third party and enable the lawyer to respond before producing the requested information;
   - has technology to withstand a reasonably foreseeable infiltration attempt;
   - addresses how confidential client information will be handled in their agreement;
   - provides the user the right to audit and obtain audit information of provider’s security procedures;
   - will host the data within a specific geographic area. If data is hosted outside the United States, the lawyer must determine that jurisdiction’s privacy laws, data security laws and protections against unlawful search and seizure are as rigorous as those in the United States and Pennsylvania;
   - provides a method for retrieving data if there is a break in service continuity;
   - provides that the lawyer may remove data from the servers for the lawyer’s own use.

136. Id.
137. Id.
138. Id. See supra note 37 and accompanying text. When addressing security issues, the Committee noted the following:

One alternative to increase security measures against data breaches could be ‘private clouds.’ Private clouds are not hosted on the Internet, and give users completely internal
Vermont

The Vermont Bar Association Professional Responsibility Section has issued an advisory ethics opinion stating that lawyers can use SaaS in connection with confidential client information “as long as they take reasonable precautions to protect the confidentiality of and to ensure access to these materials.” In light of the potential for technology to rapidly change, the opinion states it would be imprudent to establish specific conditions for SaaS use. Rather, it is noted that “the required level of due diligence will often involve a reasonable understanding of:

- the vendor’s security system;
- what practical and foreseeable limits, if any, may exist to the lawyer’s ability to ensure access to, protection of, and retrieval of the data;
- the material terms of the user agreement;
- the nature and sensitivity of the stored information;
- notice provisions if a third party seeks or gains (whether inadvertently or otherwise) access to the data; and
- other regulatory, compliance and document retention obligations that may apply based upon the nature of the stored data and the lawyer’s practice.”

The opinion stated the precautions to be taken depend on the underlying circumstances. To that end, “[t]he ability to engage in Cloud Computing is not limited by the specific location of the remote server, although . . . concerns about access to data in the event of a service interruption or an emergency, may be implicated by the location of the storage server and the extent of backup service provided by the vendor.”

security and control. Therefore, outsourcing rules do not apply to private clouds. Reasonable care standards still apply, however, as private clouds do not have impenetrable security. Another consideration might be hybrid clouds, which combine standard and private cloud functions.


140. Id. Additional matters for a lawyer to consider are:

- giving notice to the client about the proposed method for storing client data;
- having the vendor’s security and access systems reviewed by competent technical personnel;
- establishing a system for periodic review of the vendor’s system to be sure the system remains current with evolving technology and legal requirements; and
- taking reasonable measures to stay apprised of current developments regarding SaaS systems and the benefits and risks they present.

141. Id. With respect to the location of services, the opinion specifically references “choice of law clauses” as being implicated. Id.
Common Mandates Relating to Cloud Computing

When considering remote document storage in the cloud, a main concern that is raised by those who have considered the matter is the maintenance of confidentiality of client information. Keeping client information confidential is a mandate of Model Rule 1.6 and safeguarding client property is called for in Model Rule 1.15. These duties are recognized as components of competent representation under Model Rule 1.1. They inure to the lawyer, and pursuant to Model Rule 5.3, it is the responsibility of the lawyer to see that these obligations also are followed by the individuals with whom the lawyer works. With an eye toward emerging technology, including cloud computing, Ethics 20/20 proposed, and the ABA approved, amendments to the Model Rules and commentary to further these mandates. Among them is an addition to Model Rule 1.6 that highlights the need for lawyers to make reasonable efforts to prevent inadvertent or unauthorized disclosure of, or access to, client information. An extensive addition to Model Rule 1.6’s commentary is in place, giving specific direction on a lawyer’s obligation to meet this requirement. The approach taken by Ethics 20/20, and the ABA House of Delegates, is in tandem with the general path that has been taken by the States who have considered the propriety of a lawyer’s use of remote document storage.

For the most part, the opinions of the individual states that have addressed emerging technology, and cloud computing specifically, are consistent, although some “states have a higher degree of scrutiny” than others. The states that have considered the matter, along with Ethics 20/20 and the ABA House of Delegates, approve of the use of cloud computing for document storage, but call for the implementation of reasonable safeguards to protect the information and communications that are stored. Therefore the mere use of the cloud to store client material is not a breach of a lawyer’s ethical obligations, nor should it be an inadvertent waiver of any privilege that might exist. While lawyers are not called upon to guarantee the security and confidentiality of information released into the cloud, they are required to make reasonable efforts to ensure it. Arguably, this reasonable effort mirrors the reasonable precautions called for when considering inadvertent waiver under a balancing test or Fed. R. Evid. 502(b). It is the lawyer’s reasonable effort that should protect the privileged character of a communication, precluding privilege from being inadvertently waived.

142. See supra notes 55-60 and accompanying text.
143. See supra notes 62-67 and accompanying text.
145. See supra notes 110-41 and accompanying text.
146. See supra notes 70-71 and accompanying text.
147. See supra notes 99 & 101 and accompanying text.
Although storing documents on a remote server is not in and of itself an ethical breach or inadvertent waiver of privilege, the lawyer’s failure to take reasonable safeguards before doing so, could be. Mindful that technology and laws related thereto are continuing to evolve, the tendency of the states and the ABA is to shy away from specific requirements to which lawyers must adhere before accessing the cloud. 148 But while shying away from mandating specific security requirements, the various opinions have not hesitated to provide guidance on what might constitute a lawyer’s use of reasonable care. For instance, things like backing up data, implementing monitoring procedures, methods of data retrieval, and careful scrutiny of user agreement terms are among the things that a lawyer should explore before turning information over to the cloud. 149

The security or system that is appropriate in a given setting will depend on the underlying circumstances that are involved, among which are the character of the stored material and the laws that would be applicable to the stored information. Lawyers must be knowledgeable about the systems that they use, which means they must acquaint themselves with available technology, or rely on others who can make an educated determination on their behalf. This is a continuing obligation, calling for review of existing security measures, along with technological advances and applicable laws that would relate thereto. The bottom line is, when engaging in cloud services, lawyers must take the necessary steps to secure client material and protect its confidentiality. These steps are not static, but must be carefully considered and periodically evaluated, as what is “necessary” will continue to evolve. Failure to be attentive to these mandates is a breach of a lawyer’s ethical obligation, the result of which could subject a lawyer to discipline and cause significant harm to a client, such as loss of the privileged status of a communication that is considered confidential.

Conclusion

Lawyers are making use of cloud computing as a cost effective and convenient alternative to traditional hard drive storage of client material. However, with the use of this technology, which is becoming an integral part of law practice, comes significant ethical issues that must be addressed by lawyers. The ABA, and states that have considered cloud computing, approve of its use provided reasonable safeguards are taken by lawyers to secure client information and protect its confidentiality. Knowing that this is an area in which there is constant change and evolution, the tendency of entities reviewing these issues is to refrain from providing specific steps for compliance with ethical mandates, in favor of giving general guidelines for lawyers to follow. It is likely that cloud computing, as we know it today, is just a step in emerging technological innovation. As with any matter related to client information and communications, lawyers must con-

148. See supra notes 77, 111, 117, 120, 125, 131 & 140 and accompanying text.
149. See, e.g., supra notes 132 & 135 and accompanying text.
sider the underlying circumstances of a given situation when deciding what course of action is appropriate. Described as a client’s “right” and a lawyer’s “duty,” confidentiality of client information must be preserved “regardless of how much more difficult it makes [the lawyer’s] practice.”\(^{150}\) As technology changes, so will the lawyer’s use of it. The key is, regardless of what methodology is used, lawyers must employ reasonable safeguards to protect client property and maintain confidentiality of client information and communications.

\(^{150}\) Hornsby & Duffy, supra note 144.