Ethics Committee Advisory Opinion #2012-13/4
The Use of Cloud Computing in the Practice of Law

By the NHBA Ethics Committee
This opinion was submitted for publication by the NHBA Board of Governors at its February 21, 2013 meeting.

RULE REFERENCES:
Rule 1.0(e)
Rule 1.1
Rule 1.6
Rule 1.15
Rule 2.1
Rule 5.3

SUBJECTS:
Informed Consent
Competence
Confidentiality of Information
Safekeeping Property
Responsibilities Regarding Nonlawyer Assistants

ANNOTATION

The internet has changed the practice of law in many ways, including how data is stored and accessed. "Cloud computing" can be an economical and efficient way to store and use data. However, a lawyer who uses cloud computing must be aware of its effect on the lawyer's professional responsibilities. The NHBA Ethics Committee adopts the consensus among states that a lawyer may use cloud computing consistent with his or her ethical obligations, as long as the lawyer takes reasonable steps to ensure that sensitive client information remains confidential.

INTRODUCTION

As technology becomes more pervasive in the practice of law, lawyers encounter cloud computing. Cloud computing is the storage of data and the ability to run applications on remote servers over the Internet, rather than on a desktop computer or a server in a law office. Cloud computing is already a part of many devices and services which lawyers use, including smart phones, stored emails, and online data storage services such as Google Docs, Microsoft Office 365, and DropBox.1

Cloud computing offers many benefits. Typically, it is purchased on a subscription basis, usually for a monthly fee, which reduces upfront licensing costs.2 The provider takes over the responsibility for keeping up with new technology and software updates, while the lawyer enjoys access to all the data stored in the cloud from any location which has Internet access. Increased mobility and accessibility, however, may come with the loss of immediate control over the stored or transmitted data. Like any middleman, the provider of cloud computing adds a layer of risk

between the lawyer and sensitive client information.

A lawyer who uses cloud computing should therefore be aware of its effect on the lawyer's professional responsibilities. The consensus among states is that a lawyer may use cloud computing consistent with his or her ethical obligations. To date, every state bar association that has issued an opinion on using cloud computing has said that it is permissible, as long as the lawyer takes reasonable steps to ensure that sensitive client information remains confidential.3 Several rules are implicated by the use of cloud computing. This opinion discusses cloud computing, but not emails. The two are separate and raise different issues. As explained in the Pennsylvania Bar Association's opinion on cloud computing, email presents unique risks and challenges which must be addressed and mitigated separately: these include "confidentiality, authenticity, integrity, misdirection or forwarding, permanence (wanted e-mail may become lost and unwanted e-mail may remain accessible even if deleted), and malware."4

Rule 1.1. Competence

A lawyer must provide competent legal representation, and minimal competence requires a lawyer to perform the techniques of practice with skill. Rule 1.1 (b) (2). Techniques of practice include the way a client's information and the lawyer's work product are maintained, stored, and organized.5 As the revised Comment [6] to the ABA Model Rule 1.1 states, a lawyer must "keep abreast of changes in the law and its practice, including the benefits or risks associated with relevant technology."6 The comment was revised recently in response to "the sometimes bewildering pace of technological change," including cloud computing.7 A competent lawyer using cloud computing must understand and guard against the risks inherent in it.

There is no hard and fast rule as to what a lawyer must do with respect to each client when using cloud computing. The facts and circumstances of each case, including the type and sensitivity of client information, will dictate what reasonable protective measures a lawyer must take when using cloud computing. The same rationale applies to the transmission of metadata, as discussed in NH Bar Ethics Op. 2008-2009/4 on the disclosure, review, and use of metadata in electronic materials.

Competent lawyers must have a basic understanding of the technologies they use. Furthermore, as technology, the regulatory framework, and privacy laws keep changing, lawyers should keep abreast of these changes.8

Rule 1.6. Confidentiality of Information and Rule 1.0 (e). Informed Consent

Protecting client confidences is one of the most significant obligations imposed upon lawyers and is the core of the attorney-client relationship. Rule 1.6(a) states that "[a] lawyer shall not reveal information relating to the representation of a client[.]" Confidentiality applies not only to matters communicated in confidence by the client, but also to all information related to the representation, whatever its source. *See* 2004 ABA Model Rule Comment [3]. A lawyer may reveal such information if the client gives informed consent or if the disclosure is impliedly authorized. 9

As cloud computing comes into wider use, storing and transmitting information in the cloud may be deemed an impliedly authorized disclosure to the provider, so long as the lawyer takes

reasonable steps to ensure that the provider of cloud computing services has adequate safeguards. Recent revisions to Comment [16] to the ABA Model Rule 1.6 note that "if the lawyer has made reasonable efforts to prevent the access or disclosure" of confidential information, then the unauthorized access to, or the inadvertent or unauthorized disclosure of, client information does not constitute a violation of a lawyer's duty of confidentially.10

The comment sets forth a number of "[f]actors to be considered in determining the reasonableness of the lawyer's efforts" to prevent such unauthorized access or disclosure. These factors "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)."11

Not all information is alike. For example, where highly sensitive data is involved, it may become necessary to inform the client of the lawyer's use of cloud computing and to obtain the client's informed consent. "'Informed consent' denotes the agreement by a person to a proposed course of conduct after the lawyer has communicated adequate information and explanation about the material risks of and reasonably available alternatives to the proposed course of conduct." Rule 1.0 (e). The material risks and reasonably available alternatives will of course vary by client, scope of representation, the sensitivity of the stored or transmitted information, provider, and other considerations.12 But if the information is highly sensitive, consent of the client to use cloud computing may be necessary.

Rule 1.15. Safekeeping Property

"Property of clients or third persons which a lawyer is holding in the lawyer's possession," other than funds, "shall be identified as property of the client, promptly upon receipt, and safeguarded." Rule 1.15(a). The New Hampshire Supreme Court has held that the contents of a client's file belong to the client and that, upon request, an attorney must provide the client with the file. *Averill v. Cox*, 145 N.H. 328, 339 (2000). Electronic communications are also part of the client's file. NH Bar Ethics Op. 2005-06/3.

Additionally, Rule 1.16(d) of the New Hampshire Rules of Professional Conduct states that, as a condition to termination of representation, a lawyer shall "surrender[] papers and property to which the client is entitled" and only "retain papers relating to the client to the extent permitted by law." In the context of cloud computing, the lawyer must take steps to safeguard data stored in and transmitted through the cloud. What safeguards are appropriate depends on the nature and sensitivity of the data. More particularly, a lawyer must take reasonable steps to ensure that electronic data stored in the cloud is secure and available while representing a client. The data must be returned to the client and deleted from the cloud after representation is concluded or when the lawyer decides to no longer to preserve the file: in either case, the lawyer must know at all times where sensitive client information is stored, be it in the cloud or elsewhere.

Rule 5.3. Responsibilities Regarding Nonlawyer Assistants

Cloud computing is a form of outsourcing the storage and transmission of data. What was once a matter of documents and file cabinets is now online.13 This means that a provider of cloud

computing services is, in effect, a nonlawyer retained by a lawyer. As a result, the lawyer must make reasonable efforts to ensure that the provider understands and is capable of complying with its obligation to act in a manner compatible with the lawyer's own professional responsibilities. N.H. Rule 5.3 (a).

The same rationale applies when, instead of directly engaging a cloud computing provider, a lawyer hires an intermediary, such as an information technology professional or other support staff, to find and engage a provider. As noted in NH Bar Ethics Op. 2011-12/5, "Lawyers regularly engage companies to provide support services. Banks hold client funds; telephone companies carry privileged communications; credit card companies facilitate the payment of bills; computer consultants maintain necessary technology." When engaging a cloud computing provider or an intermediary who engages such a provider, the responsibility rests with the lawyer to ensure that the work is performed in a manner consistent with the lawyer's professional duties. Rule 5.3 (a). Additionally, under Rule 2.1, a lawyer must exercise independent professional judgment in representing a client and cannot hide behind a hired intermediary and ignore how client information is stored in or transmitted through the cloud.

Thus, a lawyer who uses cloud computing must take reasonable steps to ensure that sensitive client information remains confidential and secure.14 What these steps are depends on the sensitivity of the transmitted information.15 It bears repeating that a lawyer's duty is to take reasonable steps to protect confidential client information, not to become an expert in information technology. When it comes to the use of cloud computing, the Rules of Professional Conduct do not impose a strict liability standard. As one ethics committee observed, "Such a guarantee is impossible, and a lawyer can no more guarantee against unauthorized access to electronic information than he can guarantee that a burglar will not break into his file room, or that someone will not illegally intercept his mail or steal a fax."16

Which providers of cloud computing may be used and what security measures the provider must take are beyond the scope of this opinion. This opinion addresses instead what an attorney may consider when storing data on or transmitting data through the cloud. For recommendations on which cloud computing services to use, *see* American Bar Association, "Delivering Value and Efficiency with Technology: Effectively Collecting and Managing Data in a Virtual World," p. 12.17 For more information on which factors to consider when choosing a provider of cloud computing services, *see* American Bar Association, "Your ABA: Evaluating Cloud-Computing Providers."18

Cloud Computing Considerations:
The issues which an attorney must consider before using a cloud computing service include the following:

1. Is the provider of cloud computing services a reputable organization?
2. Does the provider offer robust security measures? Such measures19 must include at a minimum password protections or other verification procedures limiting access to the data; safeguards such as data back-up and restoration, a firewall, or encryption; periodic audits by third parties of the provider's security; and notification procedures in case of a breach.20

3. Is the data stored in a format that renders it retrievable as well as secure? Is it stored in a proprietary format[21] and is it promptly and reasonably retrievable by the lawyer in a format acceptable to the client? See also PA Bar Ethics Op. 2011-200, p. 9. It bears repeating that, if a client requests a copy of her file, the lawyer has an obligation to provide all files pertinent to representation of that client. NH Bar Ethics Op. 2005-06/3; *Averill*, 145 N.H. at 339-40.
4. Does the provider commingle data belonging to different clients and/or different practitioners such that retrieval may result in inadvertent disclosure?[22]
5. Do the terms of service state that the provider merely holds a license to the stored data, as for example Google's do?[23] Some providers routinely inform those accessing their service that it is the provider−not the user −that "owns" the data.[24] If the provider owns the stored data, the lawyer may run afoul of Rule 1.15, which requires that the client's property "be identified as property of the client." To comply with Rule 1.15, the provider may not "own" the data stored in the cloud.
6. Does the provider have an enforceable obligation to keep the data confidential?
7. Where are the provider's servers located and what are the privacy laws in effect at that location regarding unauthorized access, retrieval, and destruction of compromised data?[25] If the servers are located in a foreign country, do the privacy laws of that country reasonably mirror those of the United States? If the servers are relocated, will the provider notify the lawyer in advance?
8. Will the provider retain the data – and, if so, for how long – when the representation ends or the agreement between the lawyer and provider is terminated for another reason? The data must not be destroyed immediately and without notice or compromised in case of nonpayment.[26]
9. Do the terms of service obligate the provider to warn the lawyer if information is being subpoenaed by a third party, where the law permits such notice? Such a provision may be especially timely given that the Senate Judiciary Committee recently considered, but rejected legislation which would have expanded law enforcement agencies' access to privately stored data.[27]
10. What is the provider's disaster recovery plan with respect stored data? Is a copy of the digital data stored on-site?[28]

The New Hampshire Ethics Committee concurs with the consensus among states that a lawyer may use cloud computing in a manner consistent with his or her ethical duties by taking reasonable steps to protect client data. Granted, a lawyer may not find a provider of cloud computing services whose terms of service address all of the issues addressed above, but it bears repeating, that while a lawyer need not become an expert in data storage, a lawyer must remain aware of how and where data is stored and what the service agreement says.[29] Although the New Hampshire Rules of Professional Conduct do not impose a strict liability standard, the duties of confidentiality and competence are ongoing and not delegable. The requirement of competence means that even when storing data in the cloud, a lawyer must take reasonable steps to protect client information and cannot allow the storage and retrieval of data to become nebulous.

ENDNOTES:

1 American Bar Association, Cloud Computing/Software as a Service for Lawyers (last accessed on October 23, 2012). See also PA Bar Ethics Op. 2011-200 and Robinson, *Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act*, 98 Geo. L.J. 1195, 1199-1200 (2010).

2 PA Bar Ethics Op. 2011-200, p. 1.

3 AL Bar Ethics Op. 2010-02; AZ Bar Ethics Op. 09-04 (2009); CA Bar Ethics Op. 2010-179, p. 3; FL Bar Ethics Op. 06-1 (2006) ; IA Bar Ethics Op. 11-01 (2011), p. 2; IL Bar Ethics Op. 10-01 (2009), p. 3; ME Bar Ethics Op. 194 (2008); MA Bar Ethics Op. 05-04 (2005); NV Bar Ethics Op. 33 (2006); NJ Bar Ethics Op. 107 (2006); NY Bar Ethics Op. 842 (2010); NC Bar Ethics Op. 6 (2011); ND Bar Ethics Op. 99-03 (1999), p. 3; OR Bar Ethics Op. 2011-188; PA Bar Ethics Op. 2011-200, p. 1; VT Bar Ethics Op. 2003-03; VA Bar Ethics Op. 1818 (2005) .

4 PA Bar Ethics Op. 2011-200, p. 12.

5 PA Bar Ethics Op. 2011-200, p. 4.

6 In 2012, the ABA revised Comment [6] to Rule 1.1. American Bar Association Commission on Ethics 20/20, Report to the House of Delegates, Resolution, 105A Revised, p. 3 www.americanbar.org (last accessed December 27, 2012). On behalf of the New Hampshire Supreme Court's Rules Committee, the Bar's Ethics Commitee is currently reviewing the revision to Comment [6]. The proposed revision has not yet been recommended to the Rules Committee or adopted by the Supreme Court. New Hampshire Rules of Professional Conduct (last accessed December 27, 2012).

7 American Bar Association Commission on Ethics 20/20, Introduction and Overview, p. 8.

8 For example, recent Senate amendments to H.R. 2471 (2012) would have amended the Electronic Communications Privacy Act to permit warrantless searches of emails by a number of federal agencies. The amendments were introduced and then withdrawn in the face of widespread criticism, but such legislative uncertainties highlight the need to be aware of changes in technology regulation.

9*See* NH Bar Ethics Op. 2008-2009/4.

10 American Bar Association Commission on Ethics 20/20, Report to the House of Delegates, Resolution, 105A Revised, p. 5. On behalf of the New Hampshire Supreme Court's Rules Committee, the Bar's Ethics Commitee is currently reviewing the revision to Comment [16]. The proposed revision has not yet been recommended to the Rules Committee or adopted by the Supreme Court. New Hampshire Rules of Professional Conduct (last accessed December 27, 2012).

11 Id.

12 PA Bar Ethics Op. 2011-200, p. 7; IA Bar Ethics Op. 11-01 (2001), p. 2.

13 PA Bar Ethics Op. 2011-200, p. 7.

14 NH Bar Ethics Op. 2008-2009/4.

15 IA Bar Ethics Op. 11-01 (2001), p. 2.

16 N.J. Advisory Committee on Professional Ethics Op. No. 701 (electronic filing systems).

17www.americanbar.org (members of the New Hampshire Bar may contact the Ethics Committee regarding access to the article); *see also* American Bar Association, eLawyering in an Age of Accelerating Technology (last accessed January 29, 2013).

18 http://www.americanbar.org/newsletter/publications/youraba/201206article12.html (last accessed on December 3, 2012).

19 PA Bar Ethics Op. 2011-200, pp. 8-9.

20 NH law, RSA 359-C:20 (2009), already requires any person doing business in New Hampshire to notify (or cooperate in notifying) those individuals who are affected by any security breach of unencrypted computerized data that contains personal information. *See, generally*, Gallagher, Callahan & Gartrell, New Hampshire Mandates Data Breach Notification, August 2006, (last accessed on October 23, 2012).

21 Proprietary formats can only be opened by certain programs or applications. For example, Microsoft Word, which used to save word processing documents in the proprietary .DOC format now saves documents in the .DOCX format, which is supported by multiple applications. *See also* PA Bar Ethics Op. 2011-200, p. 9.

22 American Bar Association, "Cloud Computin': A Storm is A-brewin'," p. 26 (members of the New Hampshire Bar may contact the Ethics Committee regarding access to the article).

23Google Terms of Service (last modified March 1, 2012) (last accessed on December 4, 2012); *see also* MA Bar Ethics Op. 2012-03.

24 IA Bar Ethics Op. 11-01 (2001), p. 3.

25 PA Bar Ethics Op. 2011-200, p. 6.

26 IA Bar Ethics Op. 11-01 (2001), p. 3.

27 CNet, "Leahy scuttles his warrantless e-mail surveillance bill," November 20, 2012, (last accessed December 27, 2012); see also CNet, "Senate bill rewrite lets feds read your e-mail

without warrants," November 20, 2012, (last accessed December 27, 2012).

28 PA Bar Ethics Op. 2011-200, p. 10.

29 PA Bar Ethics Op. 2011-200, p. 13.