BOARD OF PROFESSIONAL RESPONSIBILITY
OF THE
SUPREME COURT OF TENNESSEE

FORMAL ETHICS OPINION 2015-F-159

May an attorney ethically store confidential client information or material in "the cloud"?

OPINION

A lawyer may ethically allow confidential client information to be stored in "the cloud" if the lawyer takes reasonable care to assure that: (1) all such information or materials remain confidential; and (2) reasonable safeguards are employed to ensure that the information is protected from breaches, loss, and other risks. Due to rapidly changing technology, the Board doesn't attempt to establish a standard of care, but instead offers guidance from other jurisdictions.

DISCUSSION

Technological advances have changed the way lawyers and law firms may store, retrieve and access client information. An inquiry has been made regarding whether a lawyer can ethically store confidential client files and information in "the cloud".

Cloud computing is technology which allows a lawyer to store and access software or data through the cloud—a remote location which is not controlled by the lawyer but by a third party which provides the storage or other computing services. It is the use of a network of remote servers, hardware and/or software to store, manage, transmit, process and/or retrieve data off the lawyer's premises, rather than on a server or personal computer on the lawyer's premises.

The services, which may be long-term storage of confidential client information or shorter-term storage or services to enable data processing or web-based email, are typically purchased from a provider on a subscription fee basis. The service provider assumes the responsibility for new technology and software updates. The lawyer's computing device is simply a way of accessing the information stored in the cloud from any location with Internet access. [1]

[1] Ala. Ethics Op. 2010-02 (2010); Alaska Ethics Op. 2014-3 (2014); Ariz. Ethics Op. 09-04 (2009); Cal. Ethics Op. 2010-179 (2010); Conn. Informal Op. 2013-07 (2013); Fla. Ethics Op. 12-3 (2012); Iowa Ethics Op. 11-01 (2011); Ky. Ethics Op. E-437 (2014); Me. Ethics Op. 207 (2013); Mass. Ethics Op. 12-03 (2012); N.H. Adv. Ethics Op. 2012-13/4 (2013); N.Y. Ethics Op. 842 (2010); Nev. Ethics Op. 33 (2006); N. C. 2011 Formal Op. 6 (2012); Ohio Informal Ethics Op. 2013-13 (2013); Or. Ethics Op. 2011-188 (2011); Penn. Formal Ethics Op. 2011-200 (undated); Va. Legal Ethics Op. 1872 (2013); Wash. Advisory Op 2215 (2012).

Because cloud computing places data, including client data, on remote servers outside of the lawyer's direct control, it has given rise to some concerns regarding its acceptability under applicable ethics rules. See "Cloud Ethics Opinions Around the U.S.", American Bar Association, Legal Technology Resource Center. This summary lists the standard of "reasonable care" with regard to the lawyer's use of cloud technology from all states supporting the use of cloud storage.

Due to the fact that technology is constantly evolving, this opinion only provides lawyers with guidance in the exercise of reasonable care and judgement regarding the lawyer's use of cloud technology in compliance with the rules of professional conduct, rather than mandating specific practices regarding the use of such technology. Ky. Ethics Op. E-437 (2014); Penn. Formal Ethics Op. 2011-200 (undated); Vt. Ethics Op. 2010-6 (2010).

Although cloud computing offers increased mobility and accessibility to client information, the placement of a service provider between the lawyer and confidential client information for which the lawyer is responsible adds a layer of risk and loss of direct control by the lawyer over the stored or transmitted information. N.H. Adv. Ethics Op. 2012-13/4 (2013). A lawyer owes the same ethical duties, obligations and protections to clients with respect to information for which they employ cloud computing as they otherwise owe clients pursuant to the Rules of Professional Conduct with respect to information in whatever form. Me. Ethics Op. 207 (2013); Ohio Informal Ethics Op. 2013-13 (2013); Penn. Formal Ethics Op. 2011-200 (undated).

Often, in house counsel has no input with regard to the technology used by the corporation, but owes the duty of communication with the corporate client regarding the risks and benefits of cloud storage. Comment 3 to RPC 1.13[2] states that when constituents of the organization make decisions for it, the decisions ordinarily must be accepted by the lawyer even if their utility or prudence is doubtful. Decisions concerning policy and operations, including ones entailing serious risk, are not as such in the lawyer's province.

Use of the technology is ethically proper if the lawyer abides by the Rules of Professional Conduct: to act competently, RPC 1.1[3], to take reasonable measures to protect the confidentiality, security,

[2] Comment [3], to RPC 1.13 provides:

> When constituents of the organization make decisions for it, the decisions ordinarily must be accepted by the lawyer even if their utility or prudence is doubtful. Decisions concerning policy and operations, including ones entailing serious risk, are not as such in the lawyer's province. Paragraph (b) makes clear, however, that when the lawyer knows that the organization is likely to be substantially injured by action of an officer or other constituent that violates a legal obligation to the organization or is in violation of law that might be imputed to the organization, the lawyer must proceed as is reasonably necessary in the best interest of the organization. As defined in RPC 1.0(f), knowledge can be inferred from circumstances, and a lawyer cannot ignore the obvious.

[3] RPC 1.1 Competence, provides:

> A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness, and preparation reasonably necessary for the representation.

and accessibility of client information stored and transmitted through the cloud, RPC 1.6[4,5,6] and 1.9(c)[7]; by competently choosing the provider of the cloud services.

The lawyer is not required by the rules to use infallible methods of protection. "When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy…" RPC 1.6, cmt. [16][6]. "…Rather, the lawyer must use reasonable care to select a mode of communication that, in light of the circumstances, will best protect confidential client information and the lawyer must advise affected parties if there is reason to believe that the chosen communications technology presents an unreasonable risk to confidentiality." Me. Ethics Op. 207 (2013); N. C. 2011 Formal Ethics Op. 6 (2012). "Special circumstances, however, may warrant special precautions." RPC 1.6, cmt. [16][6]. What safeguards are appropriate depends upon the nature and sensitivity of the data. Alaska Ethics Op. 2014-3 (2014).

Fla. Ethics Op. 12-3 (2012) states that lawyers should "consider whether the lawyer should use the outside service provider or use additional security in specific matters in which the lawyer has proprietary client information or has other particularly sensitive information."

---

[4] Rule 1.6 (a): Confidentiality of Information provides:

(a) A lawyer shall not reveal information relating to the representation of a client unless:

(1) the client gives informed consent;
(2) the disclosure is impliedly authorized in order to carry out the representation; or
(3) the disclosure is permitted by paragraph (b) or required by paragraph (c).

[5] Comment [15], Acting Competently to Preserve Confidentiality, to RPC 1.6 provides:

[15] A lawyer must act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. See RPCs 1.1, 5.1, and 5.3.

[6] Comment [16], to RPC 1.6 provides:

[16] When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule.

[7] Rule 1.9: Duties to Former Clients, provides in part:

(c) A lawyer who has formerly represented a client in a matter or whose present or former firm has formerly represented a client in a matter shall not thereafter reveal information relating to the representation or use such information to the disadvantage of the former client unless (1) the former client gives informed consent, confirmed in writing, or (2) these Rules would permit or require the lawyer to do so with respect to a client, or (3) the information has become generally known.

The duties of competence [3] and confidentiality [4, 5, 6] owed to the client by the lawyer are ongoing and are not delegable [8, 9, 10]. While competence does not require a lawyer to become an expert in data storage, it does require that the lawyer remain aware of how and where data are stored and what the provider service agreement says. Alaska Ethics Op. 2014-3 (2014).

The American Bar Association Model Rule of Professional Conduct 1.1,[11] which is identical in its wording to Rule 1.1 of the Tennessee Rules of Professional Conduct, has amended its Model Rule Comment on maintaining competence to include keeping abreast of changes "including the benefits and risks associated with relevant technology". Otherwise the comment is the same as the Tennessee version of the comment on maintaining competence.

Because the delegation of file storage to a provider of cloud computing services adds a layer between the lawyer and confidential client information over which the lawyer has responsibility, competence also requires that the lawyer ensure that tasks are delegated to competent service providers which the lawyer has selected after investigating the qualifications, competence, and diligence of the provider to ensure that client information is reasonably likely to remain confidential and secure through storage and retrieval. Ky. Ethics Op. E-437 (2014). The primary obligation is to select a reliable provider under the circumstances. In making this selection, the lawyer should consider the provider's ability to protect the information, to limit authorized access only to necessary personnel and to ensure that the information is backed up, is reasonably available

---

[8] Rule 5.1: Responsibilities of Partners, Managers, and Supervisory Lawyers, provides in part:

(a) A partner in a law firm, and a lawyer who individually or together with other lawyers possesses comparable managerial authority in a law firm, shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that all lawyers in the firm conform to the Rules of Professional Conduct.

[9] Rule 5.3: Responsibilities Regarding Nonlawyer Assistants, provides:

With respect to a nonlawyer employed, retained by, or associated with a lawyer:

(a) a partner and a lawyer who individually or together with other lawyers possesses comparable managerial authority in a law firm shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that the nonlawyer's conduct is compatible with these Rules;

(b) a lawyer having direct supervisory authority over a nonlawyer shall make reasonable efforts to ensure that the person's conduct is compatible with these Rules;

[10] Comment [1] to RPC 5.3 provides:

[1] Lawyers generally employ nonlawyer assistants in their practice, including secretaries, investigators, law student interns, and paraprofessionals. Such assistants, whether employees or independent contractors, act for the lawyer in rendition of the lawyer's professional services. A lawyer must give such assistants appropriate instruction and supervision concerning the ethical aspects of their employment, particularly regarding the obligation not to disclose information relating to representation of the client, and should be responsible for their work product. The measures employed in supervising nonlawyer assistants should take account of the fact that they do not have legal training and are not subject to professional discipline.

[11]

Maintaining Competence [8] To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, <u>including the benefits and risks associated with relevant technology</u>, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject. Underlining added.

to the lawyer and is reasonably safe from unauthorized intrusion. Alaska Ethics Op. 2014-3 (2014); Penn. Formal Ethics Op. 2011-200 (undated).

Suggested guidelines in helping lawyers competently choose the provider of the cloud services with the Rules of Professional Conduct are set forth in the following opinions:[12]

Ala. Ethics Op. 2010-02 (2010) concludes "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." The Commission defined "reasonable care" as requiring the lawyer to:

1. Learn how the provider would handle the storage and security of the data;

2. reasonably ensure that the provider abides by a confidentiality agreement in handling the data; and

3. stay abreast of appropriate safeguards that should be employed by both the lawyer and the third party.

N. C. 2011 Formal Ethics Op. 6 (2012) and Me. Ethics Op. 207 (2013) suggest that in dealing with providers of cloud computing services or hardware, lawyers should adopt additional safeguards made relevant by the Rules of Professional Conduct, such as:

1. An agreement between the cloud service provider and the lawyer or law firm that the provider will handle confidential client information in keeping with the lawyer's professional responsibilities.

2. If the lawyer terminates use of the cloud computing services or product, the provider goes out of business, or the service otherwise has a break in continuity, the law firm will have a method for retrieving the data, the data will be available in a non-proprietary format that the law firm can access, or the firm will have access to the vendor's software or source code.

3. Careful review of the terms of the law firm's user or license agreements with the provider, including the security policy.

4. Evaluation of the cloud provider's (or any third party data hosting company's) measures for safeguarding the security and confidentiality of stored data.

Pa. Formal Ethics Op. 2011-200 (undated), Maine Ethics Op. 207 (2013), N.H. Advisory Ethics Op. 2012-13/4 (2013) and Ohio Informal Ethics Op. 2013-13 (2013) listed issues which lawyers should consider before using a cloud computing service, including that the service provider:

[12] The Board is not adopting these opinions, but they are set forth as guidance to consider.

- will notify the lawyer if requested to produce data to a third party, and provide the lawyer with the ability to respond to the request before the provider produces the requested information;

- has procedures to respond to government or judicial attempts to obtain disclosure of client data;

Lawyers also need to have internal policies and procedures to aid in complying with the Rules of Professional Conduct with regard to cloud computing. Penn. Formal Ethics Op. 2011-200 (undated) and Me. Ethics Op. 207 (2013) list internal policies and procedures that lawyers should adopt in connection with cloud usage such as:

1. backing up data to allow the firm to restore data that has been lost, corrupted, or accidentally deleted;

2. educating and training employees of the firm who use cloud computing to abide by all end user security measures, including, but not limited to, the creation and regular replacement of passwords.

CONCLUSION

A lawyer may use cloud-based services with regard to confidential client information. In using cloud-based services, a lawyer must use reasonable care to assure that client confidentiality is protected and client property is safeguarded. *See,* RPC 1.6(a) and 1.9(c). A lawyer must comply with his or her duty of competence in the selection and continued use of the providers of cloud-based services. *See,* RPC 1.1. A lawyer must use "reasonable efforts" to ensure that the conduct of providers of cloud-based services is compatible with ethical obligations of the lawyer, and, if the lawyer is a partner or otherwise has managerial authority in a law firm, the lawyer must use "reasonable efforts" to make sure that the firm has measures in place to assure that providers of cloud-based services engage in conduct compatible with ethical obligations of the lawyer. *See,* RPC 5.3(a) & (b).

This 11th day of September, 2015.

ETHICS COMMITTEE:

Wade Davies

H. Scott Reams

Michael Callaway

APPROVED AND ADOPTED BY THE BOARD