ALASKA BAR ASSOCIATION
ETHICS OPINION 2014-3

CLOUD COMPUTING & THE PRACTICE OF LAW

QUESTION PRESENTED

Is it ethically permissible for a lawyer to store files in a cloud-based system and, if so, under what circumstances?

CONCLUSION

A lawyer may use cloud computing for file storage as long as he or she takes reasonable steps to ensure that sensitive client information remains confidential and safeguarded. With the issuance of this opinion, Alaska joins the community of bar associations concluding that cloud computing is permissible so long as reasonable steps to protect the client are taken.[1]

INTRODUCTION

Cloud computing is the practice of using a network of remote servers to store, manage, and process data, rather than a server in a law office or a personal computer. Typically it is purchased on a subscription basis, usually for a monthly fee. 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 with Internet access. The delegation of this file storage service to the provider of cloud computing, however, adds a layer of risk between the lawyer and sensitive client information. Because the lawyer's duties of confidentiality and competence are ongoing and not delegable, a lawyer must take reasonable steps to protect client information when storing data in the cloud.

RELEVANT AUTHORITIES

Numerous provisions from the Alaska Rules of Professional Conduct are

[1] This Ethics Opinion draws heavily from a comprehensive ethics opinion on the matter issued by the New Hampshire Bar Association. *See* NH Bar Ethics Op. 2012-13/4. *See also* AL Bar Ethics Op. 2010-02; 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).

relevant to the analysis of whether cloud computing is ethical in the practice of law.

Rule 1.1 mandates a lawyer provide competent representation, which requires legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation. Comment 6 requires lawyers to keep abreast of changes in the law and its practice.

Rule 1.6 addresses confidentiality of information. It requires that a "lawyer shall not reveal a client's confidence or secret[.]"[2] This provision is of paramount importance in the attorney-client relationship. The Rule further specifies that a "lawyer must act competently to safeguard a client's confidences and secrets against inadvertent or unauthorized disclosure by the lawyer, by other persons who are participating in the representation of the client, or by any other persons who are subject to the lawyer's supervision."[3]

Rule 1.15 requires a lawyer hold property of others with the care required of a professional fiduciary. The Rule provides that "property of clients or third persons that is in a lawyer's possession," other than funds, "shall be identified as the client's or the third person's and appropriately safeguarded."[4] Additionally, Rule 1.16(d) requires that upon termination of representation a lawyer must take steps to the extent reasonably practicable to protect a client's interest, including returning papers and property and also retaining certain papers relating to the client and the representation.

Finally, Rule 5.3 addresses the lawyer's responsibilities with respect to nonlawyer assistants. Cloud computing is a form of outsourcing that falls within the parameters of Rule 5.3. A lawyer must therefore make reasonable efforts to ensure that the provider will act in a manner compatible with the lawyer's own professional responsibilities.[5]

ANALYSIS

A lawyer engaged in cloud computing must have a basic understanding of the technology used and must keep abreast of changes in the technology.[6] A

---

[2] Rule 1.6(a).
[3] Rule 1.6(c).
[4] Rule 1.15(a).
[5] Rule 5.3(a) (requiring the lawyer to make reasonable efforts to ensure that the nonlawyer's conduct is compatible with the professional obligations of the lawyer).
[6] Commentary to Rule 1.1 (Competence) of the Model Rules of Professional Conduct was recently amended to state: "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

competent lawyer must guard against risks inherent in the practice of cloud computing. Technological changes, the regulatory framework, and privacy laws are all matters requiring the lawyer's attention.

A lawyer must take reasonable steps to ensure that the provider of cloud computing services has adequate safeguards to protect client confidences. Prior to engaging a cloud computing service, a lawyer should determine whether the provider of the services is a reputable organization. The lawyer should specifically consider whether the provider offers robust security measures. Appropriate security measures could include password protections or other verification procedures limiting access to the data, safeguards such as data backup and restoration, a firewall or encryption, periodic audits by third parties of the provider's security, and notification procedures in case of a breach.[7]

Reasonable steps must be taken to safeguard data stored in and transmitted through the cloud. What safeguards are appropriate depends upon the nature and sensitivity of the data. During the course of representation, a lawyer must take reasonable steps to ensure that the electronic data stored in the cloud are secure and available while maintaining that information on the client's behalf. If, after the representation is concluded and the decision is made not to preserve the file, then all reasonable efforts should be made to have the data deleted from the cloud as well. Otherwise, the lawyer's duty to take reasonable steps to protect the security and confidentiality of that data is ongoing. The lawyer must know at all times where sensitive client information is stored, be it in the cloud or elsewhere.

We concur with the consensus among states' ethics committees 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. While a lawyer need not become an expert in data storage, a lawyer must remain aware of how and where data are stored and what the service agreement says. Duties of confidentiality and competence are ongoing and not delegable. A lawyer must therefore take reasonable steps to protect client information when storing data in the cloud. 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.

---

lawyer is subject." *See* Model Rules of Professional Conduct 1.1, Comment 8 (emphasis added).

[7] Where highly sensitive data are involved, it may behoove a lawyer to inform the client of the lawyer's use of cloud computing and to obtain the client's informed consent. Note that the lawyer must notify the impacted client if the lawyer learns that the provider's security was breached and the client's confidence or secret was revealed. *See* Rule 5.3(d).

Approved by the Alaska Bar Association Ethics Committee on April 3, 2014.

Adopted by the Board of Governors on May 5, 2014.

G:\Ds\COMM\ETHICS\ADOPTED AK BAR ETHICS OPINIONS\2014-3.docx