Formal Ethics Opinion

KENTUCKY BAR ASSOCIATION

Ethics Opinion KBA E-437
Issued: March 21, 2014

The Rules of Professional Conduct are amended periodically. Lawyers should consult the current version of the rule and comments, SCR 3.130 (available at http://www.kybar.org/237), before relying on this opinion.

Use of Cloud Computing[1]

Question

May lawyers use cloud computing with clients' confidential information?

Answer

Yes. Lawyers may use cloud computing with clients' confidential information. In so doing, lawyers must follow the Rules of Professional Conduct with regard to

safeguarding client confidential information,
acting competently in using cloud computing,
properly supervising the provider of the cloud service, and
communicating with the client about cloud computing when such communication is necessary due to the nature of the representation.

References

SCR 3.130[Kentucky Rules of Professional Conduct] (1.1 & cmt. 6), (1.4(a) & (b)), (1.6(a) & cmt. 14, 15, & 16), (1.9(c)), (1.15(a)), (1.16), (1.18(b)), (5.3(a) & (b)); ABA Model Rules of Professional Conduct Rule 1.1, cmt. 8, Rule 1.6(c) & cmt. 18, Rule 5.3 cmt. 3; Fla. Eth. Op. 12-3(2013); Iowa Eth. Op. 11-10(2012); Me. Eth. Op. 207(2013); Mass. Eth. Op. 12-03(2012); N.H. Eth. Op. 2012-13/4(2012); N.Y. Eth. Op. 842 (2010); N.C. Eth. Op. 6 (2011); Ohio Informal Adv. Op. 2013-03(2013); Pa. Eth. Op. 2011-200(2011); Vt. Eth. Op. 2010-6(2010); Wash. Eth. Op. 2215(2012); *The Cloud and the*

[1] As another opinion states, cloud computing is "merely 'a fancy way of saying stuff's not on your computer.'" Pa. Eth. Op. 2011-200 (2011) (quoting Quinn Norton, *Byte Rights*, Maximum PC, Sept. 2012)). The National Institute of Standards and Technology (NIST) defines cloud computing 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." See Nicole Black & Matt Spiegel, *Breaking Down Cloud Computing*, available at http://apps.americanbar.org/litigation/committees/solo/articles/winter2013-0213-breaking-down-cloud-computing.html.

Small Law Firm: Business, Ethics and Privilege Considerations, New York City Bar Ass'n, Committee on Small Law Firms (Nov. 2013), available at http://www2.nycbar.org/pdf/report/uploads/20072378-TheCloudandtheSmallLawFirm.pdf; Robert Ambrogi, *High in the Cloud: Firm Central Emphasizes Integration—At a Cost,* ABA Journal p. 30(Nov. 2013); Nicole Black & Matt Spiegel, *Breaking Down Cloud Computing*, available at http://apps.americanbar.org/litigation/committees/solo/articles/winter2013-0213-breaking-down-cloud-computing.html; Sharon D. Nelson & John W. Simek, *Have Attorneys Read the iCloud Terms and Conditions?,* Slaw(Jan. 30, 2012), available at http://www.slaw.ca/2012/01/30/have-attorneys-read-the-icloud-terms-and-conditions/.

Discussion

Technology provides an ever-changing environment in which to apply the Rules of Professional Conduct. Cloud computing is technology that allows a lawyer to store and access software or data though the software or data is stored and/or operated in the cloud—that is, a remote location that is not under the control of the lawyer but is controlled by a third party who provides the storage or other service. The service may be long-term storage of confidential client information or may be shorter-term storage or services to enable data processing or web-based email.[2]

Lawyers long have had "a duty to make reasonable judgments when protecting client property and information." Pa. Eth. Op. 2011-200(2011). This duty is the same whether the lawyer is selecting a security system to protect a bricks-and-mortar law office, selecting an offsite warehouse for the storing of client files, or selecting a provider of a service such as online storage for confidential client information.

Because technology evolves every day, we decline to mandate in this opinion specific practices regarding the protection of confidential client information in the world of the cloud. The reality is that such practices soon would be obsolete—and our opinion would be obsolete as well. Rather, we choose to guide lawyers in the exercise of reasonable judgment regarding the use of cloud technology. *See* Vt. Eth. Op. 2010-6(2010) (constantly changing nature of cloud technology makes establishing "specific conditions precedent" to use not appropriate); Ohio Informal Adv. Op. 2013-03(2013) ("applying existing principles to new technological advances while refraining from mandating specific practices—is a practical one").

Use of this technology by a lawyer is ethically proper if the lawyer abides by the Rules of Professional Conduct by safeguarding client confidential information, by acting competently in using cloud computing services, by properly supervising the provider of

[2] *See* Robert Ambrogi, *High in the Cloud: Firm Central Emphasizes Integration—At a Cost,* ABA Journal p. 30(Nov. 2013)(discussing cloud-based practice management products which allow the management of cases, clients, contacts, and calendars).

the cloud service, and by communicating with the client about use of cloud services when such communication is necessary given the nature of the representation.[3]

Confidential Information and Competence

Lawyers have a duty to protect confidential client information. SCR 3.130(1.6(a)) states the basic rule that "[a] lawyer shall not reveal information relating to the representation of the client unless the client gives informed consent, the disclosure is impliedly authorized or the disclosure is permitted by paragraph (b)." The permitted disclosures of paragraph (b) are not relevant here. SCR 3.130(1.9(c)) and SCR 3.130(1.18)(b)) make clear that the duty not to reveal information relating to the representation continues to apply when the client becomes a former client and applies to prospective clients as well, even after the prospective client has moved on. *See also* SCR 3.130(1.6 cmt.16) ("The duty of confidentiality continues after the client-lawyer relationship has terminated.").

Lawyers also have a duty to act with competence. SCR 3.130(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.

Comment six to SCR 3.130(1.1) states in part that "[t]o maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice." While Kentucky's competence rule, SCR 3.130(1.1) has not been modified since 2009, the ABA, in August of 2012, amended its version of this comment to state specifically that the duty of competence includes the duty to "keep abreast" of technology.[4] While the ABA comment is not controlling, it is helpful.

Comment fourteen to SCR 3.130(1.6) clarifies that a part of the lawyer's duty of competence is 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." As with storage of files in a bricks-and-mortar law office or in an off-site warehouse, client information stored in the cloud cannot be protected absolutely. Burglars can break into law offices and warehouses despite the utmost care to protect against such happenings. Likewise, sophisticated hackers can access online information despite the utmost care to protect confidential client information.

---

[3] Many jurisdictions have issued ethics opinions dealing with cloud computing. All of them approve of lawyer use of cloud computing but provide cautionary advice. *See, e.g.,* Fla. Eth. Op. 12-3(2013); Me. Eth. Op. 207(2013); Ohio Informal Adv. Op. 2013-03(2013); Iowa Eth. Op. 11-10(2012); Mass. Eth. Op. 12-03(2012); N.H. Eth. Op. 2012-13/4(2012); Wash. Eth. Op. 2215(2012); N.C. Eth. Op. 6(2011); Pa. Eth. Op. 2011-200(2011); N.Y. Eth. Op. 842(2010); Vt. Eth. Op. 2010-6(2010).

[4] The comment to ABA Model Rule of Professional Conduct Rule 1.1 states: "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." ABA Model Rules of Professional Conduct Rule 1.1 cmt. 8.

Comment fifteen to SCR 3.130(1.6) provides:

> 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.[5]

From these statements it is clear that a lawyer has a duty to take reasonable measures to protect confidential client information in any setting: bricks-and-mortar law office, offsite warehouse, or online storage or service site in the cloud.

Taking such reasonable measures is also consistent with the duty, as stated in SCR 3.130(1.15(a)), to "appropriately safeguard[]" the client's property.

When a lawyer selects a provider of any support service, the duty of competence, the duty to protect a client's property, and the duty of confidentiality require the lawyer to investigate the qualifications, competence, and diligence of the provider. A lawyer who

---

[5] The ABA amended its version of Rule 1.6 to state that a lawyer "shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of the client." *See* ABA Model Rules of Professional Conduct Rule 1.6(c). The supporting comment language added by the ABA in August of 2012 states, in part:

> 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 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, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure. Factors to 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].

ABA Model Rules of Professional Conduct Rule 1.6 cmt. 18.

does not investigate whether a warehouse he or she is considering for the storage of files has adequate security to safeguard client files fails in his or her confidentiality and competence obligations to the client. Likewise, an attorney selecting an online provider of storage or other service must investigate the provider to be sure that client information is reasonably sure to remain confidential and secure.

Supervision

A lawyer has a duty to supervise nonlawyers engaged by the lawyer to assist the lawyer in practicing law. SCR 3.130(5.3(a)) states that with regard to a nonlawyer assistant, "[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 person's conduct is compatible with the professional obligations of the lawyer." SCR 3.130(5.3(b)) states that a lawyer with "direct supervisory authority over the nonlawyer shall make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer."

These rules require supervision of a provider of online storage just as they require supervision of an offsite provider of services such as a storage warehouse operator and just as they require supervision of a paralegal working within a bricks-and-mortar law firm. A lawyer must make "reasonable efforts" to ensure that the online storage provider's conduct "is compatible with the professional obligations of the lawyer." SCR 3.130(5.3(a)). This duty, though ongoing, is extremely important at the point that the lawyer selects the provider because it is at that point the lawyer must determine whether the provider is capable of conduct compatible with the lawyer's ethical responsibilities.[6]

Communication

SCR 3.130(1.4(a)) states that a lawyer must "reasonably consult with the client about the means by which the client's objectives are to be accomplished." While cloud computing does not always require client consultation, there may be situations in which consulting with the client may be proper. A lawyer must exercise judgment to determine if a particular client matter involves highly sensitive information such that the lawyer should consult with the client about the use of the cloud. *See also* Mass. Eth. Op. 12-03(2012)(lawyer "should refrain from storing or transmitting particularly sensitive client information by means of the Internet without first seeking and obtaining the client's express consent to do so"); N.H. Eth. Op. 2012-13/4(2012) (informing the client "may become necessary" if particularly sensitive data is at issue); Pa. Eth. Op. 2011-200(2011) (communication with client may be necessary depending on the sensitivity of the information involved and the scope of the representation).

Issues to Consider in Light of the Lawyers Responsibilities

[6] Comment three to ABA Model Rules of Professional Conduct Rule 5.3, added in August 2012, specifically notes use of "an Internet-based service to store client information" as the kind of assistance a lawyer may have.

In order to abide by these duties a lawyer owes a client, a lawyer should investigate the provider's qualifications, the provider's reputation, and the provider's longevity as well as understand the nature of the service provided. Just as a lawyer should review the terms of storage for a warehouse for storage of client files, so too should a lawyer review the terms of the arrangement[7] regarding online storage or treatment of confidential client information or other cloud-based service. Some questions that a lawyer should consider[8] in this regard include the following:

What protections does the provider have to prevent disclosure of confidential client information?

Is the provider contractually obligated to protect the security and confidentiality of information stored with it?

Does the service agreement state that the provider "owns" the data stored by the provider?[9]

What procedures, including notice procedures to the lawyer, does the provider use when responding to governmental or judicial attempts to obtain confidential client information?

---

[7] The terms often are found in the "Service Level Agreement." *See* Sharon D. Nelson & John W. Simek, *Have Attorneys Read the iCloud Terms and Conditions?*, Slaw(Jan. 30, 2012), available at http://www.slaw.ca/2012/01/30/have-attorneys-read-the-icloud-terms-and-conditions/.

[8] This list is based on a list provided by the Ohio State Bar Association. *See* Ohio Informal Adv. Op. 2013-03(2013). Florida Ethics Opinion 12-3(2013) sets forth other issues to consider:

> As suggested by the Iowa opinion, lawyers must be able to access the lawyer's own information without limit, others should not be able to access the information, but lawyers must be able to provide limited access to third parties to specific information, yet must be able to restrict their access to only that information. Iowa Ethics Opinion 11-01 also recommends considering the reputation of the service provider to be used, its location, its user agreement and whether it chooses the law or forum in which any dispute will be decided, whether it limits the service provider's liability, whether the service provider retains the information in the event the lawyer terminates the relationship with the service provider, what access the lawyer has to the data on termination of the relationship with the service provider, and whether the agreement creates "any proprietary or user rights" over the data the lawyer stores with the service provider. It also suggests that the lawyer determine whether the information is password protected, whether the information is encrypted, and whether the lawyer will have the ability to further encrypt the information if additional security measures are required because of the special nature of a particular matter or piece of information. It further suggests that the lawyer consider whether the information stored
> via cloud computing is also stored elsewhere by the lawyer in the event the lawyer cannot access the information via "the cloud."

Fla. Eth. Op. 12-3 (2013) (referring to Iowa Eth. Op. 11-10(2012)). Me. Eth. Op. 207 (2013), N.C. Eth. Op. 6 (2011), and Pa. Eth. Op. 2011-200 (2011) have other lists.

[9] SCR 3.130(1.15(a)) provides that client property must be "identified as such and appropriately safeguarded." Any statement that the service provider owns the information is inconsistent with the demands of this rule.

At the conclusion of the relationship between the lawyer or law firm and the provider, will the provider return all information to the lawyer or law firm?

Does the provider keep copies of the confidential client information after the relationship is concluded or the lawyer or law firm has removed particular client information from the provider?

What are the provider's policies and procedures regarding emergency situations such as natural disasters and power interruption?

Where, geographically, is the server used by the provider for long-term or short-term storage or other service located?[10]

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* SCR 3.130(1.6(a)) & (1.15(a)). A lawyer must act consistent with his or her duty of competence in selecting and monitoring the providers of cloud-based services. *See* SCR 3.130(1.1). A lawyer must use "reasonable efforts" to ensure that the conduct of providers of cloud-based services assisting him or her 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* 3.130(5.3(a) & (b)). Finally, a lawyer must consult with the client about the use of the cloud if the matter is sufficiently sensitive such that the duty to "reasonably consult with the client about the means by which the client's objectives are to be accomplished" is implicated. *See* SCR 3.130(1.4(b)).[11]

---

[10] Lawyers should be aware that search and seizure law as well as the law relating to ownership of information stored electronically on a server may vary greatly by country.

[11] For an in-depth but practitioner-oriented discussion of cloud use, see *The Cloud and the Small Law Firm: Business, Ethics and Privilege Considerations*, New York City Bar Ass'n, Committee on Small Law Firms (Nov. 2013), available at http://www2.nycbar.org/pdf/report/uploads/20072378-TheCloudandtheSmallLawFirm.pdf.

Note to Reader

This ethics opinion has been formally adopted by the Board of Governors of the Kentucky Bar Association under the provisions of Kentucky Supreme Court Rule 3.530. This Rule provides that formal opinions are advisory only.