OHIO STATE BAR ASSOCIATION.
EST 1880

OSBA Informal Advisory Opinion 2013-03

July 25, 2013

Re: Request for Informal Advisory Opinion

Dear _____:

You have requested the opinion of the Ohio State Bar Association Professionalism Committee on whether your law firm may use a third-party vendor to store client data in "the cloud." As you describe it, your firm currently backs up its computer files, including client documents and data, on a server located on site. You are considering a third-party vendor that is offering a program that would use "a major software provider to securely store your data off site," which your law firm would be able to access via the Internet. You indicate that the data would be encrypted before it left the law firm and would remain encrypted at the offsite data center, located in Atlanta.

The Committee's opinion is that storing client data in "the cloud" is a permutation on traditional ways of storing client data, and requires lawyers to follow the ethics rules that apply to client information in whatever form. With due regard for these rules and related Ohio ethics opinions, the Committee advises that the Ohio Rules of Professional Conduct do not prohibit storing client data in "the cloud."

Applicable Rules of Professional Conduct:

Your request for an opinion requires consideration of the following provision of the Ohio Rules of Professional Conduct ("ORPC" or "Rules"):

1.1	(lawyer shall provide competent representation);
1.4(a)(2)	(lawyer shall reasonably consult with client about means by which client's objectives are to be accomplished);
1.6(a)	(lawyer shall preserve confidentiality of information relating to the representation, subject to certain limited exceptions);
1.15(a)	(lawyer shall safeguard client property);
5.3(a)-(b)	(with respect to a non-lawyer employed by, retained by or associated with a lawyer, lawyer shall make reasonable efforts to ensure that the non-lawyer's conduct is compatible with lawyer's professional obligations).

HEADQUARTERS
1700 Lake Shore Drive
Columbus, Ohio 43204

MAILING ADDRESS
P.O. Box 16562
Columbus, Ohio 43216-6562

PHONE
614-487-2050
800-282-6556

FAX 614-487-1008
WEB www.ohiobar.org

Opinion:

The "cloud" is "merely 'a fancy way of saying stuff's not on your [own] computer.'" Formal Op. 2011-200, 1 (Pa. Bar Ass'n. Comm. on Legal Ethics & Prof'l Respon. 2011). More formally, cloud storage is the use of "internet-based computing in which large groups of remote servers are networked so as to allow ... centralized data storage." Andrew L. Askew, *iEthics: How Cloud Computing has Impacted the Rules of Professional Conduct*, 88 N. Dak. L. Rev. 453, 457 (2012).

Due to "recent advances in ... technology, the ways attorneys are able to perform and deliver legal services have drastically changed." Askew, *supra* at 466. The applicable Ohio Rules of Professional Conduct, however, are adaptable to address new technologies. Regarding cloud storage, the key rules are those relating to competent representation, communicating with the client, preserving client confidentiality, safeguarding the client's property and supervising non-lawyers that provide support services. The obligations expressed in these rules operate as they traditionally have for older data storage methods. *See, e.g.,* Adv. Op. 99-2 (Ohio Bd. of Comm'rs on Grievances & Disc. Apr. 9, 1999) (communicating by e-mail was not contemplated in 1970, when former disciplinary rule on confidentiality was adopted by Ohio Supreme Court, but "nevertheless, the rule applies" to e-mail).

The issues and ethical duties regarding cloud storage are analogous to the ones that apply when lawyers opt to use a vendor to store their paper files offsite rather than in their own offices. The analogy to paper files can help lawyers as they exercise their professional judgment in adopting specific practices that address new storage technologies such as "the cloud." That process of exercising individual judgment would not be assisted by overly-detailed regulatory input from this Committee. As one state bar ethics committee noted, a lawyer "has always been under a duty to make reasonable judgments when protecting client property and information. *Specific practices regarding protection of client property and information have always been left up to individual lawyers' judgment, and that same approach applies to the use of online data storage*," subject as always to the relevant conduct rules. Adv. Op. 2215, 2 (Wash. St. Bar Rules of Prof'l Cond. Comm. 2012) (emphasis added).

This approach – applying existing principles to new technological advances while refraining from mandating specific practices – is a practical one. Because technology changes so quickly, overly-specific rules would become obsolete as soon as they were issued. *See* Ethics Op. 2010-6 (Vt. Bar Prof'l Respon. Section 2010) (dynamism of cloud computing makes it unwise to establish "specific conditions precedent" to use). For example, rules about exactly what security measures are required in order to protect client data stored in the cloud would be superseded quickly by technological advances.[1]

---

[1] The American Bar Association's recent promulgation through the Commission on Ethics 20/20 of rule changes and new comments for the Model Rules of Professional Conduct ("MRPC") is in line with this approach. The Commission on Ethics 20/20 proposed and the ABA House of Delegates adopted minor changes to existing rules rather than specific regulations aimed at specific new technologies. *See e.g.*, revised cmt. [8] to MRPC 1.1 (lawyer should keep

Against that background, there are four main issues to consider in applying the Ohio Rules of Professional Conduct to cloud storage of client data: competently selecting an appropriate vendor; preserving confidentiality and safeguarding the client's data; supervising cloud storage vendors; and communicating with the client

1. *Competently selecting an appropriate vendor for cloud storage*

The duty of competence under ORPC 1.1 requires a lawyer to exercise the "legal knowledge, skill, thoroughness, and preparation reasonably necessary for the representation." In Ohio Advisory Opinion 2009-6 (Aug. 14, 2009), the Ohio Board of Commissioners on Grievances and Discipline ("Board") opined that a lawyer who selects a vendor for *any* type of support services that are provided outside the lawyer's firm must exercise "due diligence as to the qualifications and reputation of those to whom services are outsourced," and also as to whether the outside vendor will itself provide the requested services competently and diligently. *Id.* at 6.[2]

Knowing the qualifications, reputation and longevity of your cloud storage vendor is necessary. But in addition, just as you would review and assess the terms of a contract for off-site storage of your clients' paper files in a brick-and-mortar facility, so you must read and under-

---

up with changes in law and its practice, "*including the benefits and risks associated with relevant technology*") (emphasis added); new cmt. [3] to MRPC 5.3 (lawyer may use outside non-lawyers to assist in rendering legal services; "[e]xamples include ... *using an Internet-based service to store client information.*"; extent of lawyer's obligation to ensure that non-lawyers provide services in a manner compatible with lawyer's professional obligations "will depend upon the circumstances.") (emphasis added).

Ohio has not yet adopted any of the revised provisions of the Model Rules. *See* Univ. of Akron Miller-Becker Ctr. for Prof'l Respon., *Navigating the Practice of Law in the Wake of Ethics 20/20 - Globalization, New Technologies, and What It Means to be a Lawyer in these Uncertain Times* (Apr. 4-5, 2013), *available at* http://tinyurl.com/lblj6q8 (examining Ethics 20/20's final work and its impact in Ohio and elsewhere); Frank E. Quirk, *Lawyer Ethics for the 21st Century*, 19-21 Ohio Lawyer (Jan. - Feb. 2013) (discussing Ethics 20/20, including possible future impact on ORPC).

[2] Lawyers can call on many resources to assist in selecting a vendor. *See, e.g.*, John Edwards, *How to Pick the Best Cloud*, Law Technology News (June 11, 2013), *available at* http://tinyurl.com/k77w2sg; Nicole Black & Matt Spiegel, *Breaking Down Cloud Computing*, ABA Section of Litigation (Feb. 7, 2013), *available at* http://tinyurl.com/ksaeww8; Am. Bar Ass'n, *Moving Your Law Practice to the Cloud Safely and Ethically* (Jan. 14, 2013), *available at* http://tinyurl.com/kr3s2xw; Am. Bar Ass'n, *Evaluating Cloud-Computing Providers* (YourABA June 2012), *available at* http://tinyurl.com/l7b9wfh. *See generally*, Nick Pournader, *Embracing Technology's 'Cloudy' Frontier*, Law Practice Today (webzine of ABA Law Practice Management Section) (Oct. 2010), *available at* http://tinyurl.com/k54f3gh.

stand the agreement you enter into with an online data storage service – sometimes called a "Service Level Agreement."[3] Some commonly-occurring issues include:

- What safeguards does the vendor have to prevent confidentiality breaches?
- Does the agreement create a legally enforceable obligation on the vendor's part to safeguard the confidentiality of the data?
- Do the terms of the agreement purport to give "ownership" of the data to the vendor, or is the data merely subject to the vendor's license?[4]
- How may the vendor respond to government or judicial attempts to obtain disclosure of your client data?
- What is the vendor's policy regarding returning your client data at the termination of its relationship with your firm?
- What plans and procedures does the vendor have in case of natural disaster, electric power interruption or other catastrophic events?
- Where is the server located (particularly if the vendor itself does not actually host the data, and uses a data center located elsewhere)? Is the relationship subject to international law?

2. *Preserving confidentiality and safeguarding client property*

Under ORPC 1.6(a), a lawyer "shall not reveal information relating to the representation of a client," with only limited exceptions. As recommended by the Commission on Ethics 20/20, the ABA House of Delegates added Model Rule 1.6(c) in August 2012, requiring a lawyer to make "reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." The Ohio Supreme Court has not considered or adopted that change. Yet the language of the new Model Rule only makes explicit a duty that is already implicit in Ohio's current Rule 1.6(a). That duty is to maintain the confidentiality of all client data relating to the representation, irrespective of the form of that data, and to carry out that duty with due regard for the form that the data is in.

---

[3] *See* Sharon D. Nelson & John W. Simek, *Have Attorneys Read the iCloud Terms and Conditions?*, Slaw (Canadian online legal magazine) (Jan. 30, 2012), *available at* http://tinyrul.com/m425p3j (discussing Apple iCloud terms and conditions of use and expressing doubt that attorneys have read them).

[4] *See* § 2, below. A Service Level Agreement or terms of service that provide that the vendor "owns" the data would violate ORPC 1.15(a), which requires that client property "be identified as such" and "appropriately safeguarded."

For instance, in Advisory Opinion 99-2 (Apr. 9, 1999), the Board said that communicating with clients by e-mail was covered by the confidentiality rule in the former Code of Professional Responsibility, which "establishes a broad duty to preserve confidences and secrets that applies to all methods of communication. The duty extends to communications by electronic methods just as it extends to other forms of communication used by an attorney." *Id.* at 3. Significantly, the Board ruled that it was not necessary to encrypt e-mail communications with clients, despite the possibility that such communications might be electronically intercepted. Such a risk was not unique to e-mail in the Board's view, and did not call for extraordinary methods of protection:

> Every method of communication carries with it a risk of interception. Mail can be intercepted. Telephone messages can also be intercepted. Land-based telephones may be wiretapped, eavesdropping may occur by listening through a receiver of a telephone extension, or too loud voices may be overhead by others. Yet, these forms of communication are considered reasonable under the rule. .... To summarize, additional security measures, such as scrambling devices or encoding methods, have not traditionally been required under [the confidentiality rule] for other forms of communication frequently used by attorneys, even though the communication may be susceptible of interception.

Id. at 9-10.

Rather, the Board emphasized that "an attorney must use his or her professional judgment to determine the appropriate method of each attorney-client communication," and that client preference or particular specialized circumstances may call for taking additional measures to ensure confidentiality. *Id.* at 10-11.

In the same way, storing client data in the cloud involves yielding exclusive control over the information and puts it in the hands of a third party, just as storing a client's paper files off-site does. And similar to storing a client's paper files off-site, cloud storage raises the risk that "a third party could illegally gain access to ... confidential client data." Formal Ethics Op. 2010-02, 14 (Ala. Disc. Comm. 2010). "[J]ust as with traditional storage and retention of client files, a lawyer cannot guarantee that client confidentiality will never be breached, whether by an employee or some other third-party." *Id.* at 15. Therefore, a lawyer's duty under the ORPC to preserve the confidentiality of cloud-stored client data is to exercise competence (1) in selecting an appropriate vendor, (2) in staying abreast of technology issues that have an impact on client data storage and (3) in considering whether any special circumstances call for extra protection for particularly sensitive client information or for refraining from using the cloud to store such particularly sensitive data.

In the context of cloud storage, the requirement under ORPC 1.15(a) that client property "be identified as such and appropriately safeguarded" is a corollary to the duty to preserve the confidentiality of information related to the representation. A client's information and documents in whatever form can be construed as its "property" when in the lawyer's possession. Safeguarding such property includes reasonably ensuring that the vendor has systems in place to

protect client data from destruction, loss or unavailability. In addition, terms of service that provide or suggest that the cloud storage vendor acquires an ownership interest in the electronic data on its servers would violate the duty to keep client property "identified as such."

3. *Supervising cloud vendors*

Rule 5.3(a) of the ORPC requires that law firms make reasonable efforts to have policies and procedures in place that give reasonable assurance that the conduct of a non-lawyer employed by the lawyer is "compatible with the professional obligations of the lawyer." And under Rule 5.3(b), individual lawyers who have supervisory authority over non-lawyers must likewise make reasonable efforts to ensure that the non-lawyer's conduct is compatible with the lawyers' own professional obligations.

In its Advisory Opinion 2009-6, *supra*, the Board explained how these duties apply when lawyers outsource non-legal "support services," defined to encompass all varieties of "ministerial" services that are non-legal in nature. *Id.* at 3. The Board emphasized that while Rule 5.3's supervisory duties apply to lawyers when they outsource to support-service vendors, "the *extent* of supervision for outsourced services is a matter of professional judgment for an Ohio lawyer," subject to the requirement that lawyers exercise that judgment with the diligence due under the Rules – particularly as to the vendor's qualifications, competence and ability to protect confidentiality. *Id.* at 8 (emphasis added).

Storing client data in "the cloud" is almost by definition a service that lawyers will outsource, and cloud-storage vendors provide the kind of "ministerial" non-legal support services that are contemplated under the Board's Advisory Opinion 2009-6. Therefore, under Rule 5.3(a)-(b), lawyers who contract with a cloud-storage vendor must make reasonable efforts to ensure that the vendor's conduct is compatible with the lawyer's own professional obligations. While the extent of supervision needed is a matter of professional judgment for the lawyer, the lawyer must exercise due diligence in ascertaining whether the vendor will be capable of conduct consistent with the lawyer's own obligations.

4. *Communicating with the client*

Rule 1.4(a)(2) requires a lawyer to "reasonably consult with the client" about how the client's objectives are to be accomplished. We do not conclude that storing client data in "the cloud" always requires prior client consultation, because we interpret the language "reasonably consult" as indicating that the lawyer must use judgment in order to determine if the circumstances call for consultation. Our opinion on this point is in line with ethics authorities in other jurisdictions that have considered the question. *See, e.g.*, Formal Op. 2011-200, 5-6 (Pa. Bar Ass'n Comm. on Legal Ethics & Prof'l Respon. 2011) (not necessary to "communicate every minute detail" of representation, but it may at times be necessary to inform client of lawyer's use of cloud computing, depending on scope of representation and sensitivity of data involved); Adv. Op. 2012-13/4 (N.H. Bar Ass'n Ethics Comm. 2012) (where highly sensitive data involved, "may become necessary" to inform client and obtain consent for lawyer's use of cloud computing). In exercising judgment about whether to consult with the client about storing client data in "the cloud," the lawyer should consider, among other things, the sensitivity of the client's data.

5. *Ethics opinions from other jurisdictions regarding cloud storage*

Our conclusion that cloud storage is permissible under the ORPC is echoed by ethics authorities in other jurisdictions. To date, at least 14 states have issued ethics opinions regarding or related to cloud data storage. All have concluded that their respective lawyer conduct rules permit lawyers to store client data in the cloud, with due regard for their state ethics rules, usually their states' versions of ORPC 1.1, 1.6, 1.15 and 5.3.[5]

Conclusion:

Storing client data in "the cloud" can provide benefits to lawyers and clients by facilitating access to client data, increasing efficiency and reducing the cost of legal services. The Ohio Rules of Professional Conduct do not prohibit cloud storage, provided that lawyers follow the ethics rules that apply to client information in whatever form and are guided by applicable Ohio ethics opinions.

Sincerely,

Professionalism Committee
OHIO STATE BAR ASSOCIATION

Note: Advisory Opinions of the Ohio State Bar Association Professionalism Committee are informal, non-binding opinions in response to prospective or hypothetical questions regarding the application of the Supreme Court Rules for the Government of the Judiciary, the Rules of Professional Conduct, the Code of Judicial Conduct, and the Attorney's Oath of Office.

---

[5] The ABA has summarized and charted the opinions on cloud ethics issues via the ABA's Law Practice Management Section's Legal Technology Resource Center. *See* Am. Bar Ass'n, *Cloud Ethics Opinions Around the U.S.*, *available at* http://tinyurl.com/733gyr8.