ARTICLES

Ethical Issues Implicated by Lawyers' Use of Third-Party Cloud Services

By Amelia Toy Rudolph – February 23, 2015

Law firms increasingly turn to “cloud services” for processing and storing confidential client information because of their greater flexibility and efficiency. Use of “the cloud,” however, outsources the administration, physical control, and maintenance of sensitive data to a third-party vendor, which raises IT security and data privacy risks.

Recent amendments to the ABA Model Rules of Professional Conduct (Model Rules) indicate less leeway for lawyers who inadvertently violate their ethical obligations through the use of technology, including such ubiquitous services as cloud computing. While the cloud does not enjoy a single accepted definition, it generally encompasses a variety of products and services that provide on-demand access to remote computing services over the Internet. Cloud services can include: (1) productivity applications such as Google Docs; (2) online document and practice management software such as Rocket; (3) remote data storage, file sharing, and retrieval services such as Dropbox, Carbonite, or iCloud; and (4) web-hosted email services such as Gmail and Hotmail.

Not only can lawyers affirmatively contract with cloud service providers, but they also can access the cloud without realizing it—for example, when using their smartphones, laptops, tablets, or web conferencing services. Whether intentional or inadvertent, the use of cloud services raises a host of ethical issues for lawyers, with accompanying obligations and duties. This article reviews the ABA Model Rules relating to the use of technology, in particular the rules regarding competence, confidentiality, and outsourcing of nonlegal services, and suggests considerations for you as a lawyer to keep in mind when taking advantage of, or otherwise encountering, cloud services.

The ABA’s Ethical Rules Bearing on Technology

The ABA Commission on Ethics 20/20 was formed “to develop guidance for lawyers regarding their ethical obligations to protect [clients’ confidential] information when using technology and to update the Model Rules of Professional Conduct to reflect the realities of a digital age.” ABA Comm’n on Ethics 20/20, Report to the House of Delegates: Resolution and Report on Technology and Confidentiality (May 2012). In May 2012, the Commission submitted reports to the ABA House of Delegates regarding lawyers’ use of technology and confidentiality and regarding the ethical implications of outsourcing work on client matters to lawyers and nonlawyers outside the firm. *Id.*; ABA Comm’n on Ethics 20/20, Report to the House of Delegates: Resolution and Report on Outsourcing (May 2012).

Each state bar retains discretion as to whether and to what extent to adopt the Model Rules and recent amendments. A lawyer’s ethical obligations in a particular situation therefore depend on which state’s rules of professional conduct apply, not to mention other applicable federal, state, and international statutes, regulations, and rules regarding data privacy and security.

Rule 1.1 of the Model Rules was unchanged by the recent amendments. It 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 8 to Model Rule 1.1 was amended, however, to reinforce the importance of understanding relevant technology in order to provide competent representation to clients:

> 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.

Id. (emphasis added). While this comment would appear to expand the scope of a lawyer's duty of competence, the Commission on Ethics 20/20 report to the House of Delegates proposing the amendment states otherwise:

> The proposed amendment, which appears in a Comment, does not impose any new obligations on lawyers. Rather, the amendment is intended to serve as a reminder to lawyers that they should remain aware of technology, including the benefits and risks associated with it, as part of a lawyer's general duty to remain competent.

ABA Resolution 105A: Technology and Confidentiality (May 2012). As recent news reports of data breaches highlight, one risk associated with relevant technology is that confidentiality of data can be compromised. Rule 1.6 of the Model Rules was amended to highlight a lawyer's responsibility in this regard. Model Rule 1.6(a) states, "A lawyer shall not reveal information relating to the representation of a client" unless certain exceptions apply. Model Rule 1.6 applies to both privileged and nonprivileged but confidential client information. The ABA added a new provision, Model Rule 1.6(c):

> A lawyer shall make *reasonable efforts* to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.

Id. (emphasis added). Although this duty was already described in several existing comments to Model Rule 1.6, the rule was amended to state this obligation explicitly in the black-letter rule, given the pervasive use of technology to store and transmit confidential client information. A new comment to Model Rule 1.6, Comment 18, provides further guidance on what is required for a lawyer to act competently to preserve confidentiality and makes clear that this amendment was

not intended to create a strict liability standard for lawyers any time a client's confidentiality is breached:

> 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. 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.

Id. (citations omitted). Another Model Rule affected by technology-related amendments isModel Rule 5.3, Responsibilities Regarding Nonlawyer Assistance. While the black-letter rule was unchanged, the comments to the rule were significantly revised to clarify the professional obligations of a lawyer outsourcing legal and nonlegal work within and outside the firm. In particular, a new Comment 3 to Model Rule 5.3 identifies the distinct concerns that arise when nonlegal services are performed outside the firm that involve technology:

> A lawyer may use nonlawyers outside the firm to assist the lawyer in rendering legal services to the client. Examples include the retention of an investigative or paraprofessional service, hiring a document management company to create and maintain a database for complex litigation, sending client documents to a third party for printing or scanning, and using an Internet-based service to store client information. When using such services outside the firm, a lawyer must make reasonable efforts to ensure that the services are provided in a manner that is compatible with the lawyer's professional obligations. The extent of this obligation will depend upon the circumstances, including the education, experience and reputation of the nonlawyer; the nature of the services involved; the terms of any arrangements concerning the protection of client information; and the legal and ethical environments of the jurisdictions in which the services will be performed, particularly with regard to confidentiality. When retaining or directing a

> nonlawyer outside the firm, a lawyer should communicate directions appropriate under the circumstances to give reasonable assurance that the nonlawyer's conduct is compatible with the professional obligations of the lawyer.

Id. (citations omitted).

Application of the ABA Ethical Rules to Cloud Services

As soon as a lawyer gives a third party access to his or her clients' information—whether a copy service, an offsite storage facility, or a cloud service provider—that lawyer risks the loss of confidentiality. As discussed above, Model Rule 1.1 requires lawyers to obtain the requisite level of knowledge and understanding of the technology they use to understand and manage the risks triggered by the use of that technology. This includes taking reasonable precautions to ensure that the technology they use is adequate and consistent with their professional obligations. The following are potential risks that you, as a lawyer, should take into account when dealing with cloud services.

To paraphrase the adage, security begins at home. Your own access to the cloud should be secure, whether wired or wireless. Not only should the cloud service facility be secure, but your point of access should also be secure, as well as your means of transmission to and from the cloud. If you use portable devices such as smartphones, laptops, or tablets, those devices should be internally secured so that the data stored on them remains protected in case of loss or theft. Many law firms have implemented BYOD (bring your own device) policies, and you should ascertain whether your firm has such a policy and, if so, comply with it.

If you are using the cloud to transmit or store client information, you have two main categories of risks to consider: first, risks associated with the cloud service provider itself and any unauthorized third parties attempting to access your client data through that provider, and second, risks associated with your own ability to access client data from your provider as needed. To assess these risks, Comment 3 to Rule 5.3, discussed above, would recommend that you read the service agreement from the cloud service provider to understand the extent to which these risks are implicated by the service you have chosen. It may also be advisable, if not required (*see, e.g.*, Office of the Comptroller of the Currency,OCC Bull. No. 2013-29, Risk Management Guidance (Oct. 30, 2013)), to document the due diligence you perform regarding your chosen cloud service provider, in case your judgment is second-guessed later. This due diligence is not a one-time event, but should be undertaken at regular intervals to ensure that your understanding of the cloud service remains up-to-date.

Your obligations regarding use of the cloud for client data can be heightened if circumstances indicate greater sensitivity of the data—for example, if your clients are subject to the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act, or the Fair Credit Reporting Act; if your client's information is controlled for export; or if you are handling very sensitive litigation or working on a confidential proposed transaction. In such

circumstances, Model Rule 1.1 may require client consent to the use of cloud services. Your client engagement letters may also require you to notify the client of use of cloud services.

10 Important Considerations in Use of Cloud Services

These are 10 issues to consider when evaluating your cloud service provider:

(1) Is the provider reputable, experienced, and well-established? Does the provider have experience in protecting confidential and sensitive information? Is the provider likely to remain in business for the foreseeable future?

(2) What security measures and protocols does the provider have in place to prevent reasonably foreseeable confidentiality breaches, either by its own employees or by unauthorized third parties? For example, does the provider have firewalls, encryption, robust passwords, intrusion detection systems, employee background checks, and other similar protocols? Does the provider conduct periodic audits to monitor the effectiveness of its protocols? Does the provider regularly update these protocols to be consistent with current best practices, as they evolve to match the ingenuity of hackers?

(3) Is the provider relying on any third parties to maintain or support its servers? If so, who are those third parties, and what is their competence and experience in handling confidential or sensitive information?

(4) Where are the provider's servers located? You will need to know which laws govern those servers and, in particular, whether any international or foreign privacy laws might apply to your client data stored on such servers. For the same reason, if the provider is relying on third parties to support its service, you will need to know where those third parties are located.

(5) Is the provider obligated to notify you promptly in the event of a confidentiality breach, and how does the service agreement define "promptly"? You have obligations of your own in the event of a data breach affecting one or more of your clients, which can vary from state to state; will your provider notify you in enough time for you to comply with your obligations?

(6) What does the service agreement provide with regard to ownership and licensing of data stored with your provider? The service agreement may be unclear or inappropriate regarding who owns or has the right to use the data stored with the provider. In this regard, remember that Model Rule 1.15 requires that client property be identified as property of the client. If you direct the provider to produce or provide access to client information stored with the provider, can the provider refuse to comply with that direction pending resolution of a dispute over billing or other matters? What is your right of access to client information stored with the provider pending such a dispute?

(7) What are the provider's obligations in responding to subpoenas or other government or civil process? Is the provider obligated to notify you if it is served with process requiring production of your client's information, and, if so, is that notice required to be provided in sufficient time to permit you to intervene and object to the subpoena? Is the provider empowered to resist production if appropriate and permissible?

(8) What happens to your stored data when the relationship between your firm and the provider ends? What is the provider's obligation to return custody of the data to you and to purge and wipe any copies of the data on its servers? What are the provider's obligations if it is bought or sold, if it goes into bankruptcy, or if it shuts down for any other reason?

(9) Does the service agreement allow your provider to unilaterally modify its privacy and acceptable use policies without notice to you?

(10) What is your recourse if something goes wrong? Does the provider's service agreement contain a disclaimer or limitation of liability provision?

The answers to these questions are as varied as the service agreements themselves. But knowing the answers will help you to assess knowledgeably the risks associated with the cloud service you are considering and to take reasonable precautions against unauthorized breaches of confidentiality, consistent with your ethical obligations.

Keywords: litigation, commercial, business, technology, cloud services, confidentiality, data, ethics, Model Rule 1.1, Model Rule 1.6, Model Rule 1.16, Model Rule 5.3

Amelia Toy Rudolph is with Sutherland Asbill & Brennan LLP in Atlanta, Georgia.