Managing Partner Forum®
ADVANCING THE BUSINESS OF LAW

THE ETHICS OF CLOUD COMPUTING FOR LAWYERS

by

Nicole Black
My Case

FEATURED ARTICLE

POWERED BY
TheRemsenGroup
Smart Strategies for the Forward Thinking Law Firm
TheRemsenGroup.com

Managing Partner Forum®
ADVANCING THE BUSINESS OF LAW

The Ethics of Cloud Computing for Lawyers

By Nicole Black

Cloud computing, where your data and software are stored on servers owned and maintained by a third party, once an unfamiliar and foreign concept, is becoming increasingly commonplace. As a result, lawyers are seeking to take advantage of the many benefits of using cloud computing services in their law practices, including cost savings, flexibility, and agility.

Of course, many ethical issues arise when lawyers seek to store confidential client data on servers to which third parties have access. It's not surprising, then, that over the last few years a number of ethics committees have wrestled with the ethical issues presented when lawyers seek to use cloud computing in their law practices. Those committees have released the following opinions: North Carolina State Bar Council 2011 Formal Ethics Opinion 6, Massachusetts Bar Association Ethics Opinion 12-03, Oregon State Bar Formal Opinion No. 2011-188, Professional Ethics Committee of the Florida Bar Op. 10-2 (2011), New York State Bar Association's Committee on Professional Ethics Op. 842 (2010), Pennsylvania Bar Association Ethics Opinion No. 2010-060 (2010), and Iowa Committee on Practice Ethics and Guidelines Ethics Opinion 11-01 (2011).

Thus far, US ethics commissions have determined that it is ethical for lawyers to use cloud computing, with most concluding that lawyers must take reasonable steps to ensure that their law firm's confidential data is protected from unauthorized third party access.

The Iowa opinion, Ethics Opinion 11-01, handed down in September 2011, is illustrative and offers a well-balanced and thorough analysis of a lawyer's ethical obligations when using cloud computing platforms to store confidential client data. In it, the committee concludes:

> (A 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.

The Committee also provided a detailed and thorough list of suggested questions that lawyers should ask all technology vendors, not just cloud computing providers. The questions focus on assisting lawyers in assessing the accessibility and security of their data stored in the cloud:

- Will I have unrestricted access to the stored data?
- Have I stored the data elsewhere so that if access to my data is denied I can acquire the data via another source?
- Have I performed due diligence regarding the company that will be storing my data?
- Is it a solid company with a good operating record, and is its service recommended by others in the field?
- In which country and state is it located, and where does it do business?
- Does its end user's licensing agreement (EULA) contain legal restrictions regarding its responsibility or liability, choice of law or forum, or limitation on damages?
- Likewise, does its EULA grant it proprietary or user rights over my data?
- What is the cost of the service, how is it paid, and what happens in the event of nonpayment?
- In the event of a financial default, will I lose access to the data, does it become the property of the SaaS company, or is the data destroyed?
- How do I terminate the relationship with the SaaS company?
- What type of notice does the EULA require?
- How do I retrieve my data, and does the SaaS company retain copies?
- Are passwords required to access the program that contains my data?
- Who has access to the passwords?
- Will the public have access to my data?
- If I allow nonclients access to a portion of the data, will they have access to other data that I want protected?
- Recognizing that some data will require a higher degree of protection than other data, will I have the ability to encrypt certain data using higher level encryption tools of my choosing?

The state bar associations aren't alone in their efforts to address the ethical implications of lawyers using cloud computing services. In fact, the American Bar Association recently addressed the ethics of cloud computing during its Annual Meeting in early August 2012. The ABA House of Delegates approved resolutions that incorporated updates to the Model Rules of Professional Conduct relating to cloud computing.

First, Model Rule 1.6, which addresses lawyers' duties when dealing with confidential information, was amended to include a newly added subdivision (c), which requires lawyers 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 commentary to this new subdivision sets forth suggested factors to be considered when assessing the risks of unintended disclosure of confidential information, including 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).

The commentary to Model Rule 5.3, which addresses lawyers' responsibilities when using nonlawyer assistance, was also amended. The commentary suggests that when lawyers use third-party nonlawyer providers, such as cloud computing services, 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.
In other words, both the ABA and the state ethics committees that have addressed the ethics of cloud computing use by lawyers thus far have given cloud computing their blessing. Lawyers can ethically use cloud computing products in their law practices. But before doing so, it is imperative that they fully assess their ethical obligations and exercise due diligence in vetting their cloud computing provider of choice.

For a full list of the ethics opinions from the various jurisdictions, you can refer to an online chart recently published by the ABA. This handy chart compares and contrasts the different holdings and can be found here.

# # #

About the Author

Nicole Black
Nicole Black is a Rochester, New York attorney and Director of Business and Community Relations at MyCase, web-based law practice management software. She's been blogging since 2005 and the author of Cloud Computing for Lawyers. She can be reached at niki.black@mycase.com.