

THE DAILY RECORD

WESTERN NEW YORK'S SOURCE FOR LAW, REAL ESTATE, FINANCE AND GENERAL INTELLIGENCE SINCE 1908

LegalCURRENTS

Maintaining confidentiality in the information age

Maintaining the confidentiality of digital data — it's an ever-present conundrum for lawyers as cloud computing increases in popularity and mobile use becomes ubiquitous.

In fact, for many lawyers, the thorny ethical issues presented by these technologies, including housing client data on servers owned and maintained by others, is one of the main reasons behind their reluctance to use cloud computing products in their practices.

The lack of guidance from bar associations, caused in large part by the relative newness of the technologies, has also contributed to hesitancy regarding cloud computing. It's only been over the past few years that a handful of ethics committees have issued decisions regarding the use of cloud computing products and lawyers' obligations in regard to client data stored in the cloud or on mobile devices.

Overall, the opinions, have reached similar conclusions centered around requiring lawyers to make reasonable efforts to maintain confidentiality when storing client data on third-party servers, whether cloud-based or not. See, for example, Professional Ethics Committee of the Florida Op. 10-2 (2011), North Carolina Bar Proposed 2011 Formal Ethics Opinion 6 (2011), New York State Bar Association's Committee on Professional Ethics Op. 842 (2010), Arizona State Bar Committee on Rules of Professional Conduct, Opinion 09-04 (2009), N.J. Supreme Court Advisory Comm. on Prof'l Ethics, Op. 701 (2006) and Nev. State Bar Standing Comm. on Ethics & Professional Responsibility Formal Op. 33 (2006).

So, although the list isn't extensive, the number of jurisdictions that have considered these issues is slowly, but surely, increasing. In fact, it appears that additional guidance is on the horizon — this time from the American Bar Association's Commission on Ethics 20/20.

As I explained in past columns, this committee was established in 2009 (online at www.abanet.org/ethics2020) and the

stated purpose of the commission is to “perform a thorough review of the ABA Model Rules of Professional Conduct and the U.S. system of lawyer regulation in the context of advances in technology and global legal practice developments.”

Last week, the committee released its initial draft proposals (which are available for further comment through July 15) regarding a number of different issues, including confidentiality when outsourcing, which I'll discuss in next week's column, and confidentiality-related obligations when using technology, which I discuss below.

The committee is proposing that Rule 1.6 of the ABA Model Rules of Professional Conduct, which addresses confidentiality of information, be amended and that subsection (c) be added to the rule. The proposed subsection (c), which mimics the language used by other jurisdictions that have addressed this issue, reads as follows:

- (c) A lawyer shall make reasonable efforts to prevent the inadvertent disclosure of, or unauthorized access to, information relating to the representation of a client.

The proposed comment that would follow the new subsection explains what steps a lawyer must take in order to meet the obligation of making “reasonable efforts” to maintain confidentiality:

- Acting Competently to Preserve Confidentiality

Paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer or other persons or entities who are participating in the representation of the client or who are subject to the lawyer's supervision or monitoring. See Rules 1.1, 5.1 and 5.3.

Factors to be considered in determining the reasonableness of the lawyer's efforts include the sensitivity of the information, the likelihood of disclosure if additional safeguards are not

Continued ...



By **NICOLE BLACK**

Daily Record
Columnist

THE DAILY RECORD

WESTERN NEW YORK'S SOURCE FOR LAW, REAL ESTATE, FINANCE AND GENERAL INTELLIGENCE SINCE 1908

Continued ...

employed, and the cost of employing additional safeguards. 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.

This rule comports with the conclusions reached by other jurisdictions and provides useful guidance in the form of a broadly framed, elastic standard that assists attorneys in making careful choices about the technologies that best fit their individual practices.

All in all, this proposed rule is encouraging and I applaud the

committee for their efforts.

Next week, I'll discuss the committee's recommendations regarding maintaining confidentiality when outsourcing tasks related to client matters, which includes the use of cloud computing services, so stay tuned.

*Nicole Black is of counsel to Fiandach & Fiandach in Rochester. She co-authors the ABA book *Social Media for Lawyers: the Next Frontier*, co-authors *Criminal Law in New York*, a West-Thomson treatise, and is currently writing a book about cloud computing for lawyers that will be published by the ABA in early 2011. She is the founder of *lawtechTalk.com* and speaks regularly at conferences regarding the intersection of law and technology. She publishes four legal blogs and can be reached at nblack@nicoleblackesq.com.*