Monday, September 26, 2011

THE DAILY RECORD

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

LegalCURRENTS

# Pa. rules on lawyers using cloud computing

Is it ethical for lawyers to store and access confidential client data in the "cloud" using computers or mobile devices? As more lawyers become familiar with, and use, these technologies, this question is slowly, but surely, being asked of ethics committees across the country.

As I've discussed in prior columns, both Florida and New York ethics committees have addressed this issue and each concluded that lawyers can use cloud computing services to store confidential client data as long as reasonable steps are taken to ensure that client confidentiality is maintained. (See, Professional Ethics Committee of the Florida Bar Op. 10-2 [2011] and New York State Bar Association's Committee on Professional Ethics Op. 842 [2010]).

By NICOLE BLACK
Daily Record Columnist

The American Bar Association's Committee on Ethics 20/20 is also in the process of tackling this issue and has proposed that Model Rule 1.6, which addresses lawyers' duty to maintain confidential information, be revised to add the following section to the rule, which mirrors the language used by the Florida and New York ethics committees: "(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."

Meanwhile, the North Carolina Bar has not yet issued a formal opinion and continues to struggle with this issue, having issued two proposed opinions on the ethical obligations of lawyers who choose to use cloud computing platforms in their practice, the most recent of which is the North Carolina Bar Proposed 2011 Formal Ethics Opinion 6 (2011).

And, in January 2011, the Pennsylvania Bar Association chimed in on the subject, issuing Ethics Opinion No. 2010-060, which addressed two inquiries:

(1) Can an attorney ethically allow client confidential material to be stored in "the cloud" by the software manufacturer?

(2) Are there ethical considerations regarding the use of Smartphones, in general and particularly in regard to those that are synchronized through "the cloud" and data can be remotely removed through the phone?

The conclusion reached was quite similar to the New York and Florida committees' conclusions: Yes, lawyers may use these technologies, provided that they take appropriate measures to ensure that the confidentiality client data is not breached.

The author of the opinion explained that taking steps to maintain confidentiality was of paramount importance: "Because cloud computing refers to 'offsite' storage of client data, lawyers must be aware of and take appropriate precautions to prevent compromising client confidentiality, i.e., attorneys must take great care to assure that any data stored offsite remains confidential and not accessible to anyone other than those persons authorized by their firms."

The opinion also provided lawyers with a useful list of issues to consider and steps to take when choosing and utilizing cloud computing platforms. Importantly, it was noted that these security measures are equally applicable to the traditional law office setting: "[A]n attorney using cloud computing is under the same obligation to maintain client confidentiality as is the attorney who uses non-online documents management ..." and "the [security] measures ... will vary based upon the technology and infrastructure of each office."

The suggested issues to factor into a decision to move to the cloud include:

- Backing up data to allow the firm to restore data that has been lost, corrupted, or accidentally deleted;
- Installing a firewall to limit access to the firm's network;
- Limiting information that is provided to others to what is required/needed/requested;
- Avoiding inadvertent disclosure of information such as Social Security numbers;
- Verifying the identity of individuals to whom the attorney provides confidential information;

*Continued ...*

Monday, September 26, 2011

THE DAILY RECORD

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

*Continued ...*

• Refusing to disclose confidential information to unauthorized individuals (including family members and friends) without client permission;

• Protecting electronic records containing confidential data, including backups, by encrypting the confidential data;

• Implementing electronic audit trail procedures to monitor who is accessing the data; and

• Creating plans to address security breaches, including the identification of persons to be notified about any known or suspected security breach involving confidential data.

All in all, the Pennsylvania opinion is an example of a forward-thinking application of existing rules and allows lawyers the flexibility to determine which tools are most appropriate for their particular practice. This decision is wisely based on the premise that although the tools may be changing, lawyers' ethical obligations remain the same.

New technologies don't warrant new, more stringent rules or requirements, but rather require the careful, thoughtful application of existing rules while leaving lawyers a wide berth to take advantage of emerging tools and technologies.

*Nicole Black is of counsel to Fiandach & Fiandach in Rochester. She co-authors the ABA book Social Media for Lawyers: the Next Frontier, coauthors 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. 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.*