

THE DAILY RECORD

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

NYSBA Ethics Committee weighs in on the cloud

My column last week detailed the American Bar Association's Commission on Ethics 20/20 call for comments regarding cloud computing.

I disagreed with the commission's suggestion that attorneys may be obligated to "supervise" their cloud computing provider's provision of services.

A reader expressed concern that my position might cause attorneys to believe they have no obligation to understand or research the cloud computing services prior to using them. He raised a good point, and that wasn't my intent. My position regarding attorneys' obligations regarding emerging technologies is quite the opposite.

My discussion in that column was limited specifically to the issue of whether lawyers have an obligation to supervise software developers in the day-to-day administration of a legal software platform, given that most lawyers lack the technical skills necessary to do so.

In fact, in prior columns and writings, and in the book on cloud computing I'm in the process of writing (to be published by the ABA in early 2011), I repeatedly stress that attorneys have an obligation to stay abreast of changing technologies and take reasonable efforts to ensure their clients' data will be secure if housed in the cloud.

Interestingly, in September, the New York State Bar Association's Committee on Professional Ethics addressed this very issue in Opinion 842. Specifically, the committee considered the issue of whether an attorney can use an online system to store confidential client data and, if so, what steps must be taken to ensure the data are secure. In other words, the committee squarely addressed the ethics of using cloud computing platforms in a law practice.

All in all, the opinion was favorable, and very helpful, to attorneys interested in the possibility of using cloud computing services in their law firms.

The committee concluded it is permissible for attorneys to store confidential client data in the cloud, but only if reasonable steps are taken to ensure the data would be adequately protected from unauthorized disclosure: "A lawyer may use an online data storage system to store and back up client confidential information provided that the lawyer takes reasonable care to ensure that confidentiality will be maintained in a manner consistent with the lawyer's obligations under Rule 1.6. In addition, the lawyer should stay abreast of technological advances to ensure that the storage system remains sufficiently advanced to protect the client's information, and should monitor the changing law of

privilege to ensure that storing the information online will not cause loss or waiver of any privilege."

Importantly, the committee noted that "exercising 'reasonable care' under Rule 1.6 does not mean that a lawyer guarantees that the information is secure from any unauthorized access."

In other words, as I've often repeated, reasonable security measures do not ensure absolute security. Absolute security is an absolute impossibility — and it's heartening that the committee acknowledged that reality in its opinion.

The committee also provided very helpful guidance for lawyers, explaining the steps they should be taken to ensure client data will be sufficiently protected. Lawyers should:

- Be certain the cloud provider has an enforceable obligation to preserve confidentiality and security, and that the provider will notify the lawyer if served with process requiring the production of client information;
- Investigate the provider's security measures, policies, recoverability methods and other procedures to determine if they are adequate;
- Employ available technology to guard against reasonably foreseeable attempts to infiltrate the data; and/or
- Investigate the provider's ability to purge and wipe

any copies of the data, and move data to a different host if the lawyer becomes dissatisfied or otherwise wants to change providers.

So, as the NYSBA's committee rightfully concluded, and as I've repeatedly stated in the past, lawyers cannot blindly utilize cloud computing technologies without first understanding and researching the services provided by the cloud computing provider.

Exercising reasonable care entails asking the right questions and ensuring the provider's responses assure you that your clients' confidential information will be reasonably protected from unintended disclosure.

*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.*



By **NICOLE BLACK**

Daily Record
Columnist