Monday, April 18, 2011

THE DAILY RECORD

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

LegalCURRENTS

# Cloud computing and the encryption red herring

Recently, I've encountered a number of people who claim that the only way lawyers can responsibly use cloud computing services in their law practice is if all files are encrypted before sending them to the cloud.

This claim is based on the fear that employees of the cloud computing provider will have access to the law firm's unencrypted data stored on the cloud computing provider's servers.

By NICOLE BLACK
Daily Record Columnist

This blanket assertion is, quite frankly, ridiculous. Lawyers routinely outsource the handling and storage of confidential client data in paper form — from third-party document storage warehouses to process servers to delivery services. And, there has never been a requirement to lock the documents in fireproof safes, encode or otherwise encrypt those documents in order to prevent third parties from viewing them.

Not to mention that lawyers have been sending confidential client documents and data via unencrypted email for over a decade now. In fact ethics committees in multiple jurisdictions concluded many years ago that, in most cases, attorneys may use unencrypted email without violating their ethical obligation to maintain client confidentiality.

See, for example, N.Y. State 709 (1998), State of Maine Ethics Opinion #195 (2008), American Bar Association Formal Opinion No. 99-413, Ohio Ethics Opinion No. 99-2 (April 9, 1999), Hawaii Ethics Opinion No. 40 (April 26, 2001), Utah Ethics Opinion No. 00-01 (March 9, 2000), Florida Ethics Opinion No. 00-4 (July 15, 2000), Delaware Ethics Opinion No. 2001-2 (2001), and Virginia Ethics Opinion No. 1791 (Dec. 22, 2003).

Importantly, just last fall, in N.Y. Ethics Op. 842, the New York State Bar Association's Committee on Professional Ethics concluded that it is permissible for attorneys to store confidential client data in the cloud, as long as reasonable steps are taken to ensure the data would be adequately protected from unauthorized disclosure. Nowhere to be found in the opinion is the requirement that all documents be encrypted.

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

Of course, that doesn't mean that attorneys should carte blanche store any and all client data in the cloud. Some attorneys may choose to utilize the cloud for backup storage by uploading only non-confidential data into the cloud, including legal forms, administrative forms, redacted memos of law for future reference and excerpts from legal research.

Others may choose to choose to test the cloud computing waters by using cloud computing services for tasks that don't require the input of confidential information, such as billing or time tracking.

Still other attorneys may choose to store unencrypted, confidential client data in the cloud, but only after exercising due diligence, asking the appropriate questions of cloud computing providers (which I've discussed more in depth in previous columns) and ensuring that the provider's responses are sufficient to ensure that confidential client information will be reasonably protected from unintended disclosure.

Finally, other attorneys may choose to store only encrypted data in the cloud or forego cloud computing altogether. This determination may revolve around the ethics rules of the jurisdiction in which the attorney practices and the types of data at

*Continued ...*

Monday, April 18, 2011

THE DAILY RECORD

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

*Continued ...*

issue. Some attorneys may conclude, after assessing their practice areas and the types of clients that the represent, that their clients' data is extremely sensitive and that the risk of disclosure by third parties is high.

This may occur where the client is a well-known celebrity or the data consists of highly sought after trade secrets. Or, it may be that the attorney is simply uncomfortable with the idea of storing client data in the cloud.

The bottom line is that lawyers can use cloud computing without encrypting the files before storing them in the cloud. That being said, the determination of whether to upload unencrypted client data into the cloud will vary from one law practice to another and is contingent upon the type of data that will be housed in the cloud.

*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.*