THE DAILY RECORD

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

Does cloud computing compromise clients?

I predict that within about two to three years, lawyers in most jurisdictions will communicate and collaborate with clients using some type of an encrypted network.

A number of states, including Massachusetts and Nevada, already have passed laws or regulations requiring certain types of confidential data to be sent electronically only via encrypted communications. More laws of that nature most certainly will follow, both at the state and federal level.

In my opinion, such laws — most of which apply primarily to financial institutions — ultimately will incorporate some of the types of client information contained in attorney-client communications, in large part because of rising concerns due to recent large-scale data disclosures.

In fact, that type of data breach is one of the primary reservations expressed by lawyers when considering whether to implement cloud computing platforms in their law practice.

A recent federal court decision fanned the fire, causing many attorneys to decry the use of cloud computing and assert that doing so violated the very basic obligation to protect confidential client communications and data.

By NICOLE BLACK
Daily Record Columnist

In a decision issued last week by the U.S. District Court for District of Oregon, in *In re U.S.*, Nos. 08-9131-MC, 08-9147-MC, the government argued successfully that it need not notify the account holder regarding a warrant served on the ISP holder of the e-mail account. In reaching its decision, the court gave lip service to the concept that e-mails are entitled to Fourth Amendment protections, but then stated: "Much of the reluctance to apply traditional notions of third-party disclosure to the e-mail context seems to stem from a fundamental misunderstanding of the lack of privacy we all have in our e-mails. Some people seem to think that they are as private as letters, phone calls, or journal entries. The blunt fact is, they are not."

In comparison, however, see footnote 7 from the October Memorandum and Order issued by the U.S. District Court, Eastern District of New York, in *U.S. v. Cioffi*: "One preliminary matter is not in question: The government does not dispute that Tannin has a reasonable expectation of privacy in the contents of his personal e-mail account." *See U.S. v. Zavala,* 541 F3d 562,577 (Fifth Circuit 2008) ('[C]ell phones contain a wealth of private information, including emails, text messages, call histories, address books, and subscriber numbers. [The defendant] had a reasonable expectation of privacy regarding this information.'); *U.S. v. Forrester,* 512 F3d 500, 511 (Ninth Circuit 2008) ('E-mail, like physical mail, has an outside address 'visible' to the third-party carriers that transmit it to its intended location, and also a package of content that the sender presumes will be read only by the intended recipient. The privacy interests in these two forms of communication are identical. The contents may deserve Fourth Amendment protection, but the address and size of the package do not.')."

Accordingly, despite the fact the dicta in the Oregon decision flies in the face of binding precedent, online commentators repeatedly raised concerns regarding the decision, asserting it was further evidence that the use of cloud computing in law practices is ill-advised.

I would assert to the contrary the Oregon dicta is further evidence that the incorporation of encrypted client communications in cloud computing may well be the primary factor that convinces attorneys to accept cloud computing services as a legitimate law practice management alternative to traditional software packages.

A number of well-established cloud computing providers already incorporate encrypted communications in their platforms. For example, VLOTech, Clio and NetDocuments allow for varying types of encrypted communication with clients. Another online legal platform, NKrypt, is devoted to providing a secure, encrypted e-mail network.

Cloud computing providers are adapting quickly to and responding to the concerns raised by lawyers. As a result, lawyers are becoming increasingly comfortable with the concept of cloud computing. In fact, according to the 2009 Am Law Tech Survey, 84 percent of responding law firms already use SaaS (Software as a Service), a form of cloud computing, in some capacity.

As cloud computing becomes more prevalent in the legal field, more lawyers will understand the importance of carefully negotiating their contracts with the services providers to ensure that, for example, they are notified if a warrant relating to their data is served.

Mark my words: Cloud computing is the wave of the future, and encrypted communication is one of the keys to putting attorney's minds at ease re- garding an emerging technology. Astute providers will incorporate encrypted communication into their platforms, and smart lawyers will learn about and use the emerging technology in their practice.

Nicole Black is of counsel to Fiandach and Fiandach and is the founder of lawtechTalk.com, which offers legal technology consulting services, and publishes four legal blogs, one of which is Practicing Law in the 21st Century (http://21stcenturylaw.wordpress.com). She may be reached at nblack@nicoleblackesq.com.