THE DAILY RECORD

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

Should lawyers be wary of SaaS?

Online services for lawyers are becoming increasingly common and, for many lawyers, are an attractive alternative to the traditional law practice management software installed and maintained on a local server within a law office.

Online services available to attorneys now include law practice management systems, document management platforms, secure email networks, digital dictation services and billing/timekeeping services. The online platforms are attractive, economical and viable alternatives for firms of all sizes.

Online e-mail platforms also are increasing in popularity. Yahoo, Hotmail and Gmail now are the top three e-mail service providers in the United States, and are used by lawyers and clients alike.

The one thing these various platforms have in common is that the data created and managed by these services are stored offsite, in the "cloud." The offsite data storage issue has resulted in much speculation among lawyers regarding issues of data security and attorney-client confidentiality.

By NICOLE BLACK
Daily Record Columnist

Before addressing those concerns, let's define the concepts at issue.

"Cloud computing" is a "type of computing that is comparable to grid computing, relies on sharing computing resources rather than having local servers or personal devices to handle applications. The goal of cloud computing is to apply traditional supercomputing power (normally used by military and research facilities) to perform tens of trillions of computations per second."

Software as a service — or SaaS — is defined at Oracle.com as "[a] software delivery model in which a software firm provides daily technical operation, maintenance, and support for the software provided to their client."

In my opinion, the data security and confidentiality concerns regarding cloud computing are exaggerated and overblown.

Of course an attorney has an obligation to research how an SaaS provider will handle confidential information, and should determine how securely the data is stored. It is important to ensure the company stores the data on servers that meet current industry standards, performs back-ups regularly, and that you are satisfied data will not be lost should a catastrophic event occur.

Concerns that third parties could access the data while traveling through the "cloud" are downright silly, in my opinion. Third parties always have had access to confidential client information, including process servers, court employees, document processing companies, external copy centers and legal document delivery services.

Employees of the building in which a law office is located also have had access to confidential files, including the cleaning service and other employees who maintain the premises. What about summer interns, temporary employees and contract attorneys?

The employees who manage and have access to computer servers are no different. In order to practice law effectively, third parties necessarily must have access to certain files. Assurances that the company in question will make reasonable efforts to ensure employees will not access confidential information is all that's required.

The New York State Bar Association Committee on Professional Ethics reached a similar conclusion in Opinion 820-2/08/08, where it answered: "May a lawyer use an e-mail service provider that scans e-mails by computer for keywords and then sends or displays instantaneously (to the side of the e-mails in question) computer-generated advertisements to users of the service based on the e-mail communications?"

The committee concluded: "Unless the lawyer learns information suggesting that the provider is materially departing from conventional privacy policies or is using the information it obtains by computer-scanning of e-mails for a purpose that, unlike computer-generated advertising, puts confidentiality at risk, the use of such e-mail services comports with DR 4-101. … A lawyer may use an e-mail service provider that conducts computer scans of e-mails to generate computer advertising, where the e-mails are not reviewed by or provided to other individuals."

In other words, common sense prevails. Lawyers must resist the urge to overreact to emerging technologies.

Common sense dictates that the same confidentiality standards applicable to physical client files likewise apply to computer-generated data. To conclude otherwise would be to prohibit lawyers from using computers in their law practices — an unrealistic and, quite frankly, ridiculous alternative.

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@nicole-blackesq.com.