LEGAL TECHNOLOGY

Ethics Committees And Cloud Technology —Can They Get Along?

By **Cindy Wolf, Esq.**
SPECIAL TO LAW WEEK COLORADO

CLOUD COMPUTING is one of the most popular and least understood computing trends. Lawyers have joined it, some without realizing it. They use cloud-based email, store and backup documents and photographs online, and use other systems that require them to log in to the Internet to access their data on a vendor's server.

Is this a problem? As lawyers like to say, that depends. There are no ethics opinions regarding cloud computing in Colorado, but there are ethics rules to consider: 1) the requirement to keep client information confidential and 2) maintenance of the attorney-client privilege.

Other states, including New York, New Jersey, North Carolina, Nevada, Pennsylvania, Arizona, Iowa and Alabama, as well as the American Bar Association have issued opinions on whether lawyers can store client information in the cloud. They all start off with a resounding "Yes" as long as lawyers use "reasonable precautions" in choosing a system that protects their clients' data. This is where reality and ethics committees part ways. Many of the recommendations are impossible to

CINDY WOLF

follow. They may sound innocuous, but to anyone who has negotiated with a cloud vendor (and you are lucky if they will do so), they are laughable.

Email and other forms of electronic data

Let's talk about email. The American Bar Association has issued a few opinions on this topic that leave much to a lawyer's judgment. In 1999, it said unencrypted email was a safe method of communication because there was a reasonable expectation of privacy — and yes, cloud based email was available back then. The opinion goes on to say, however, that if the lawyer doesn't think there is a reasonable expectation of privacy (remember communication has at least two participants, and the lawyer only controls one end), the lawyer has a duty to notify the client and get his or her consent before using email, or the lawyer should cease email with the client. Maintenance of the attorney-client privilege with email, as with any communication, takes additional steps depending upon many variables.

Electronic data storage in the cloud is a separate, yet related issue. Let's take a look at some of the "best practices" recommended by the brave ethics committees willing to tackle the issue.

First, lawyers should keep current on the technologies to understand whether their cloud provider's system is sufficient to protect their client's information. Clearly due diligence is important. But, few lawyers have the technical ability to do security audits of data center(s) and electronic service delivery programs and then compare those practices to the latest industry standards. So, this requirement implies that lawyers must either have an unlikely level of technical expertise or hire a specialist to do an investigation of a proposed provider—and then regularly update that investigation.

Next, lawyers are cautioned not to hire any provider that disclaims or limits its liability for its own errors or omissions. Such disclaimers and limits are standard in cloud provider contracts. Some cloud providers may be willing to negotiate on this issue, but the cloud provider that accepts full liability needs a better lawyer.

In an expansion of the liability theme, lawyers are also told to confirm that the provider will assume legal liability for the confidentiality of the data. North Carolina even recommends that you request the provider's employees to act as your fiduciary in this respect (*Really*?). It isn't ridiculous to ask for a confidentiality obligation in a cloud contract, although they are not popular for general-purpose applications (such as iCloud or Google Documents). But cloud providers will not guarantee absolute security that would be necessary for full liability for confidentiality. And then there are those pesky limitations of liability.

Additional concerns

Some cloud provider practices can cause other problems for lawyers. To have flexible storage capacity and use systems efficiently, providers typically have more than one data center and use them as needed. There are several reasons you should know the physical address where your data resides. If your client's data contains technology subject to export control, you will have to handle the export compliance.

Larger providers may have multiple data centers, sometimes in many parts of the world. They often can't tell you which data center will house your data. While some providers will not balk at a requirement to keep data in the U.S. (provided they can technically do that), Pennsylvania, for example, recommends that the provider guarantee that the data will never leave the state.

Having data in different states can create conflicts of law issues and potential logistical problems, but clearly that ethics committee wasn't thinking about how this requirement would affect lawyers with a multi-state practice.

Certain types of law practice bring up special problems in the cloud. If you have protected health, financial, student or personal information in your client data, you also have to worry about the extra electronic-security requirements contained in HIPAA, FERPA, other federal and state laws and credit card processing rules. Ethics committees sometimes think to bring this up. And seriously, don't even consider most U.S. based providers if you have European personally identifiable information in your data.

What's a lawyer to do?

One approach suggested by the ABA and some insurance carriers is to get the client's informed consent to use the cloud. This covers a lawyer under Colorado Rules of Civil Procedure Rule 1.6 client confidentiality requirements. But what is "informed" consent? Would all risks of disclosure need to be disclosed like the risks of anesthesia and other medical procedures? Can you adequately identify and quantify them?

So, the real question is, what are you doing in the cloud? Do you run your practice on Clio or Nextpoint? Do you use iCloud or Google Documents for client related documents? Do you know where your data is? Does your provider at least agree to keep your data confidential?

The cloud is a variable and dynamic place. It is maturing as an industry—even as hackers are working hard to subvert it. Though Colorado has yet to opine, you would be wise to proceed there only with reasonable precautions. Do your investigations. Get your client's informed consent. Only deal with stable, reputable vendors. Negotiate reasonable terms — that alone eliminates a lot of the competition. •

— Cindy Wolf is a Colorado lawyer with more than 25 years of experience representing large and small domestic and multinational companies. Her expertise is commercial contracting with an emphasis on technology licensing and the Internet She can be reached and cwolf.esq@gmail.com..