LEGAL MANAGEMENT
THE MAGAZINE OF THE ASSOCIATION OF LEGAL ADMINISTRATORS

Who Owns Your Data When It's in the Cloud?

The cloud makes things vastly simpler for law firms: Important information can be stored and synced across multiple devices. It's easier for IT to support. You can access just about anything you need no matter where you or what device you have on hand.

JOE KELLY
Founder and CEO
Legal Workspace

But before you take advantage of free storage options, think twice.

As tempting as iCloud, Google Drive, Dropbox or other sites may be, there are ownership complications that can arise from uploading confidential or privileged information to these types of free and low-cost services. These sites are geared toward consumers — not law firms — and it may not be clear where the data resides or whether users surrender their ownership rights to information in that particular cloud.

WHO OWNS THE DATA?

With free and low-cost services, attorneys may not even own their intellectual property after they upload it. Terms of ownership can vary across sites such as Google Drive, Dropbox, Apple's iCloud and Microsoft's SkyDrive.

Clicking "agree" to long-winded service agreements and uploading data often means that users automatically abide by the provider's terms. As Microsoft says on its ***Services Agreement page***: "By using or accessing the Services, or by agreeing to these terms where the option is made available to you in the user interface, you agree to abide by this Agreement without modification by you. If you don't agree, you may not use the Services."

These services may not cost money, but that doesn't mean they are actually free. Consider that Google sells ads based on the data it collects, which means someone at the company is looking at the data. Many of these sites also retain the right to determine whether data is offensive or violates copyright or IP law. For example, Apple reserves the right to delete any information in iCloud that it finds objectionable.

If the information resides in countries with different privacy laws than the United States, lawyers may also find themselves with cross-border jurisdictional headaches.

HOW SECURE IS THE DATA?

Data breaches are a distressingly common occurrence. When hackers can penetrate the online defenses of highly sophisticated companies and publicize their sensitive business information, you should rightfully worry about the security of consumer-grade storage. If users have questions about security features and approaches, it may be difficult to find someone at the provider's organization who can answer questions thoroughly and knowledgeably.

These types of storage approaches are often associated with emails that require few login steps. If a user has her Gmail account stored on her smartphone and then loses the phone, whoever finds it may have an easy time accessing all the files connected to the cloud through that email address.

WHERE IS THE DATA?

Users should not be surprised that data on a cloud can be located anywhere. Google alone operates data centers in South Carolina, Iowa, Georgia, Oklahoma, North Carolina, Oregon, Chile, Taiwan, Singapore, Finland, Belgium, Ireland and Netherlands.

If attorneys need to find their data quickly, it may be far more time-consuming than they initially expect. If the information resides in countries with different privacy laws than the United States, lawyers may also find themselves with cross-border jurisdictional headaches.

FINDING THE RIGHT PROVIDER

While free or cheap cloud providers may seem like a bargain in the short term, they can be very costly in the long run if data is left vulnerable, especially when law firm attorneys and staff have unwittingly surrendered their ownership rights to information.

When looking at cloud providers, consider the following:

- **Thorough security protocols:** While free and low-cost services certainly try to keep data secure, it may be difficult to find out exactly what protocols, firewalls and operating systems are in place to protect information.

- **Legal-specific software and infrastructure:** Free cloud services are easy to use, but they may not integrate well with the other tools and software the firm uses. This means that data may be difficult to access and merge with the other technology.

- **Trained and vetted staff:** It may be difficult for users to find out which cloud service employees have physical and virtual access to their data and what background checks have been performed on those employees. Likewise, what happens if there are technical problems? If an attorney has trouble getting data in the cloud, finding someone to help could be a serious issue. There may also be little recourse if the data cannot be recovered.

"Free" doesn't always equate to inexpensive. Lawyers looking for cloud storage options should be willing to pay a little more for enterprise-grade, legal-specific data storage. Otherwise, they may find out too late that they don't truly own their data or that someone else has taken it.

ABOUT THE AUTHOR

Joe Kelly, Founder and Chief Executive Officer of Legal Workspace, formally launched the company in 2010. In 2006, he first saw the potential for the Legal Workspace solution because of his broad exposure to how law firms operate. The evolution of virtualization, connectivity and hosting

technologies made Legal Workspace a commercially viable solution, and it went live with its first client firm in 2008.

Email
LinkedIn
Twitter
Blog
Website