

Owning Your Data in the Cloud

When deciding which cloud service to use for clients' information, keep in mind that the trade-off for free or low-cost service might be minimal security and loss of control over location and even ownership of the data.

JOE KELLY

As many law firms are discovering, the cloud can be a wonderful business tool. With cloud services, lawyers on the go can access their data wherever they are, on their preferred devices. They aren't tethered to the office or cumbersome physical servers.

Some sites even offer free storage, which may be conveniently tied to email or smartphones. Yet as tempting as iCloud, Google Drive, Dropbox, or other sites may be, lawyers need to do their research first before uploading their important, confidential, or privileged information to these types of free and low-cost services.

Many of these sites are geared toward consumers, not law firms. Such sites may lack key security provisions, and it may not be clear where the data resides or whether users surrender their ownership rights to information in that particular cloud.

When weighing whether to use a cloud provider for any type of information storage, lawyers have a responsibility to know where their data is, feel confident that it won't be lost or stolen, and understand who truly owns it.

Who Owns the Data?

With free and low-cost services, lawyers might 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 extremely 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 “free” services may not cost money, but that doesn’t mean they are truly 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 intellectual property law. For example, Apple reserves the right to delete any information in iCloud that it finds objectionable.

According to Apple’s service terms: “However, Apple reserves the right at all times to determine whether Content is appropriate and in compliance with this Agreement, and may pre-screen, move, refuse, modify and/or remove Content at any time, without prior notice and in its sole discretion, if such Content is found to be in violation of this Agreement or is otherwise objectionable.”

How Secure is the Data?

Data breaches are becoming a distressingly common occurrence. When hackers can penetrate the online defenses of highly sophisticated companies and publicize their most sensitive business information, lawyers should rightfully worry about the security of consumer-grade storage. If users have questions about security features and approaches, it may be difficult to even 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 log-in steps. If a user has her Gmail account stored on her smartphone and accidentally loses it, whoever finds the phone may have an easy time accessing all the files connected to the cloud through that email address.

Where is the Data?

With something called the “cloud,” users should not be surprised that data 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 the Netherlands. If lawyers 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 Cloud 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 or lawyers have unwittingly surrendered their ownership rights to their own information. Law firms would be better off paying a little more for legal-specific cloud providers to get the security and peace of mind they need.

When looking at different cloud providers, there are several things to consider.

Thorough Security Protocols. While free and low-cost services certainly try to keep data secure, it may be difficult for lawyers, or any user, to find out exactly what protocols, firewalls, and operating systems are in place to protect information.

It may also be difficult for users to find out which employees have physical and virtual access to their data and what background checks have been performed on those employees.

Legal-specific Software and Infrastructure. While many of these cloud services are easy to use, 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. When lawyers using free cloud storage have questions, they may not know who to contact for information. It may also be difficult to determine the level of training and expertise of those they do speak with. If a lawyer has trouble getting data in the cloud, finding someone who can help could be a serious issue. There may also be little recourse if the data cannot be recovered.

Conclusion

“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. For more information about cloud storage options, login to wisbar.org and visit [Practice411™](#) – the State Bar of Wisconsin Law Office Management Assistance Program. And, plan to attend “Let’s Be Reasonable: Ethics & Cybersecurity” during the State Bar [Annual Meeting & Conference](#), June 15-17, 2016.

This article appeared in Bloomberg BNA’s Big Law Business, April 14, 2015.

About the Author

Joe Kelly, founder and CEO of Legal Workspace, launched his company after seeing the potential for the cloud in law firm operations. He is also the founder of Business Network Consulting, Ltd., which implements and supports IT solutions for mid-market companies.

This article appeared in the March 2016 issue of Wisconsin Lawyer, the official publication of the State Bar of Wisconsin. Used with permission.

<http://www.wisbar.org/NewsPublications/WisconsinLawyer/Pages/Article.aspx?Volume=89&Issue=3&ArticleID=24680>