
3 Questions To Ask When Considering the Cloud

By Joe Kelly, founder and CEO, Legal Workspace

While the cloud may offer scalable and mobile technology opportunities, many of the non-legal-specific sites attorneys may automatically turn to (think iCloud, Google Drive or Dropbox) may lack key security provisions. Additionally, it may not be clear with these sites where confidential or privileged information 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 legal information storage, attorneys 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. Here are three questions you should always ask when it comes to the cloud and data ownership.

1. Who owns the data?

With free and low-cost services, attorneys may not own their intellectual property after they upload it. Terms of ownership varies across sites like 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 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 IP law. For example, Apple's service terms includes a section that states that it reserves the right to delete any information in iCloud that it finds objectionable.

2. How secure is the data?

Data breaches are becoming a distressingly common occurrence. 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 free or non-legal specific cloud storage approaches are often associated with emails that require few log-in steps. If a user has a Gmail account stored on his/her smart phone 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.

3. Where is the data?

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 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.

Joe Kelly, founder and CEO 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.

Originally published April 14, 2015 by Bloomberg BNA Big Law Business

© 2015 Legal Workspace