

LTN Law Technology News

ALM Properties, Inc.

Page printed from: [Law Technology News](#)

[Back to Article](#)

Backing Up Documents in the Cloud

John Edwards

Law Technology News

08-04-2011

Cloud backup services, which store files on internet-based servers, can take much of the pain out of creating and maintaining document backups. Cloud storage allows attorneys to transfer essential files to a secure, remote location almost as soon as they are created, virtually eliminating any possibility of losing an important file to accidental erasure or a natural or man-made calamity.

The downside is that cloud computing is still an emerging technology, which can make it difficult for an attorney to find a high-quality service that's both efficient and cost-effective. Here's some advice to help you cut through the cloud computing fog:

SERVICES

The various cloud backup services are taking different approaches to online storage. Some companies, like [Mozy](#), offer users proprietary client software that monitors files or folders stored anywhere on the user's computer and automatically backs the items up whenever they change.

[Dropbox](#), on the other hand, requires users to place files and/or folders into a special computer-based folder that automatically syncs into the cloud. If anything happens to the user's computer and its files, the data located in the Dropbox folder can be retrieved simply by reconnecting to the service. Dropbox can also be used to sync files on multiple devices, including laptops, smartphones, and tablets.

One of the biggest benefits is the anywhere, anytime access. "This is especially important for lawyers who work around the clock and need access to their information at any hour," says Courtney Kaufman, a manager at [Accent Computer Solutions](#), an IT services provider located in Rancho Cucamonga, Calif. "Whether you're at your desk, on your laptop, smartphone, or tablet, you have access to the same information and you'll be fully working."

[SugarSync](#), meanwhile, offers a kind of hybrid service that offers both automatic syncing across multiple user devices as well as client software that watches over files and folders located anywhere on the user's computer.

Yet another cloud backup alternative is [Amazon Simple Storage Service](#) (Amazon S3), which, despite its name, isn't particularly simple to use. To backup data with Amazon S3, users need to open an account and create a "bucket" (which is how S3 describes a storage folder). Next, the user has to find S3-compatible backup software and supply it with the unique public and private keys required to use the service. For most lawyers, Amazon S3's complexity negates any possible financial benefit.

COST

Cloud storage is generally more expensive on a per-gigabyte basis than physical media backup technologies such as portable drives, DVDs, and memory sticks and cards. Dropbox.com, for instance, charges \$200 a year for 100GB of online storage. Mozy.com is cheaper, offering 125GB of storage for approximately \$120 per year. In both cases, the costs for a specific amount of storage is ongoing, unlike physical media, which is purchased once and is likely to last for many years.

SECURITY

Virtually all cloud backup providers use data encryption -- typically Advanced Encryption Standard technology at a 128-, 192- or 256-bit security level -- to safeguard sensitive information from internal and external snoops. Therefore, as long as one uses a secure password and carefully protects it, the chance of a hacker or other unauthorized party accessing a cloud-stored file is very small.

Even with provider-supplied safeguards, the burden of assuring the existence of cloud adequate security falls squarely upon the attorney using the service, says Jim Kunick, chair of the intellectual property and technology group at Much Shelist, a Chicago law firm. He points to the ABA's Formal Ethics Opinion 95-398, which states: "A lawyer who gives a computer maintenance company access to information in client files must make reasonable efforts to ensure that the company has in place, or will establish, reasonable procedures to protect the confidentiality of client information. Should a significant breach of confidentiality occur, the lawyer may be obligated to disclose it to the client."

But cloud providers don't always make it easy for attorneys to ensure client data safety or privacy. Dropbox, for instance, made headlines in June over [a nearly four-hour data breach that the company claimed affected fewer than 100 accounts, as well as a perceived lax attitude toward customer data privacy](#).

PRIVACY

Rajesh Goel, chief technology officer at [Brainlink International](#), a New York-based compliance security consulting firm, warns that storing data in the cloud could, under some circumstances, pose a privacy risk to client data. "If a firm is large enough and they have the financial and technical resources to build their own private cloud, then the advantages of cloud computing are compelling," he says. "For firms lured by the low cost/save money siren song of public and hybrid clouds, there's danger ahead."

Goel observes that while the Electronic Communications Privacy Act assures that e-mail has a 180-day right to privacy, information held in databases has zero days of privacy protection. "All online applications ... can be classified as databases, under the strict definition of ECPA," Goel asserts.

Goel says that attorneys also need to be aware of another potential privacy threat. "The Patriot Act allows law enforcement to use National Security Letters to obtain information about individuals and companies from service providers," he says. "Most NSLs forbid the service provider from notifying their clients that they have released information to law enforcement, based on NSLs."

Goel adds that lawyers with clients in highly regulated areas, such as health care and financial services, also need to fully investigate their situation and privacy risk potential before sending files into the cloud.

RELIABILITY

While cloud backup services are highly reliable, and users are far less likely to lose data to a cloud snafu than to damaged or lost physical media, problems occasionally surface. [Carbonite](#), for example, experienced a hardware failure in 2009 that resulted in some 7,500 customers losing access to their stored data, some permanently.

Perhaps most essential to cloud reliability, particularly with a sync-type service such as Dropbox, is having a fast and steady internet connection. "If your internet connection is lost (to a cloud syncing service), you won't be able to work," Kaufman observes. "The upside here, though, is that because your information is cloud-based, you can go to any wireless hotspot and you're back in business."

BOTTOM LINE

Cloud backup services provide a safe and convenient alternative to traditional data backup technologies, but at a higher cost, with some potential cost disadvantages, and reliability and privacy risks.

John Edwards is a freelance writer based in Arizona. E-mail: jedwards@gojohnedwards.com

Copyright 2011. ALM Media Properties, LLC. All rights reserved.