ONLINE DATA STORAGE PROVIDERS

ONLINE STORAGE GENERALLY

An online data storage provider is an Internet-based service that backs up your entire system automatically, and stores the data on the Internet in a secure form and location. You may see this process referred to as storing your data "in the cloud," Web-based data storage, or "software as a service" (SaaS).

Using Internet-based data storage for backup and recovery has generated significant discussion in legal circles. Before deciding to use a third party to store your electronic data, review the following:

- OSB Formal Opinion No. 2011-188,
- Safeguarding Client Information in a Digital World by Helen Hierschbiel, *Oregon State Bar Bulletin* (July 2010),
- The Ethics of Electronic Client Files: Floating in the Cloud by Amber Hollister, *Oregon State Bar Bulletin* (May 2017), and
- Understanding Security When Using Cloud Storage by Hong Dao, *InPractice* (October 20, 2017).

The data stored on your computer is the lifeline of your practice. Safeguarding that information is critical to your practice's survival, and to meeting your ethical obligations to your clients. Online data storage can provide access to, and protection of, your data that an offsite backup cannot. This is especially true if your offsite backup is stored in your same town or locale and a natural disaster strikes. A backup device at home or other local site would likely be inaccessible or damaged. In contrast, if you are displaced from your office by a localized disaster, Internet-based data storage allows you access to client documents and financial information as soon as you are able to access the Internet.

Despite potential advantages, many lawyers have reservations about using online data storage. Generally, security issues associated with storage are the main concern. Placing client information in the hands of third parties, the solvency of the provider, the security of the storage location, the method of storage, and the preservation of confidentiality are all reasonable concerns raised by lawyers. However, these concerns exist whether you store paper files in a storage facility or store electronic data with an online provider. With a paper storage facility, once you are confident the facility has no access to your stored documents or maintains your confidentiality and privacy, you turn over the boxes of client files for storage and periodic retrieval. Placing electronic client data in the hands of third parties who remotely upload it to their website is not any different. Proper security is crucial for each storage method. Unauthorized access can happen if a paper storage or an electronic storage site is not secure.

Similar to a physical storage center, an online storage center can provide the user with a special key to access electronically stored data. An online provider's security can be so restrictive that the user may be the only person who has the key. Storage this restrictive requires careful thought, planning, and safeguarding, as there is no access if the key is lost. Therefore, if you are the only key holder, store the key (usually a password) locally somewhere that is secure, such as a safe deposit box, as well as somewhere secure in another geographic area. Do not rely on your memory.

ONLINE DATA STORAGE PROVIDERS

Vet the Vendor

When choosing an online data provider for storage or backup, consider asking the vendor the following questions:

- Does the system offer the highest form of data encryption available in the United States: Advanced Encryption Standard (AES)?
- Does the system offer a private encryption key, held only by your office?
- Does the system encrypt all transmitted data at the source?
- Is data encrypted both at rest and in transit?
- Does the system provide continuous, automatic backups?
- Does the system have the capability to back up time-sensitive data like open files, emails, and databases?
- Does the system provide full coverage for complete data protection and recovery, including backup, offsite storage, ability to restore data over the network or dedicated storage device, online remote recovery, and offline archiving and recovery?
- Does the system provide instant file restores 24 hours a day, 7 days a week, 365 days a year?
- Does the system provide automatic notification of exceptions or problems encountered?
- Does the system provide detailed activity reports?
- Is the online data server in a geographic location that is separate from your locale?
- Does the online data storage provider take precautions for disasters in its own area, such as backing up on a server in another location?
- Is the online data storage provider's physical site secure? (The highest level of security is a Tier One Data Center Facility.)
- Is there a secure way for your firm to access the stored information, if someone loses the law firm encryption key?
- What access does the cloud service provider have to your data? Be sure to review the Terms of Service (TOS) or End User Licensing Agreement (EULA) or Service Level Agreement (SLA). Make no assumptions.
- Does the cloud service provider actually store your data, or is it stored elsewhere? Review any agreement between the cloud service provider and its data storage facility. Make no assumptions.

Online Data Storage:

- Carbonite
- CrashPlan
- FilesAnywhere
- Iron Mountain
- LiveVault
- Backblaze
- SpiderOak

See also, How to Back Up Your Computer, available online at https://www.osbplf.org/. (Select Practice Management, and then select Forms.)

NOTE: This information does not constitute an endorsement of or recommendation for a particular product or vendor. Technology changes over time. Attorneys should conduct their own appropriate research before using technology, and continue to review hardware and software over time. Attorneys who choose to use third-party online data storage should also review OSB Formal Opinion No. 2011-188.

ONLINE DATA STORAGE PROVIDERS

IMPORTANT NOTICES