TECHNOLOGY UPDATE

The Cloud, The Cloud—How Secure Is It?

By Joseph G. Hodges, Jr., Esq.

Ever since the invention of the concept of the "cloud" for the storage of technology data, allegedly by Joseph Carl Robnett Licklider in the 1960s, cloud computing (otherwise known as **Software as a Service**) has developed along a number of lines, with Web 2.0 being the most recent evolution. However, since the internet only started to offer significant bandwidth in the 1990s, cloud computing for the masses has been something of more recent vintage.

According to Wikipedia (http://en.wikipedia.org/wiki/Cloud_storage), cloud storage is a model for networked enterprise storage where data is stored in virtualized pools that are generally hosted by third parties. Hosting companies operate large data centers, and people who require their data to be hosted buy or lease storage capacity from them. The data center operators, in the background, virtualize the resources according to the requirements of the customer and expose them as storage pools, which the customers can themselves use to store files or data objects. Physically, the resource may span across multiple servers and multiple locations. The safety of the files depends upon the hosting companies, and on the applications that leverage the cloud storage. Cloud storage services may be accessed through a web service application programming interface (API) or by applications that utilize the API, such as cloud desktop storage, a cloud storage gateway or Web-based content management systems.

Choosing the best cloud storage provider is a tough decision, as there are so many options available online. To assist in this regard, www.TheTop10BestOnlineBackup.com (2014) has created a website that contains reviews of over 50 of the world's leading cloud storage devices that allows users to add comments and feedback about their experiences with them so others can make an informed decision on the best cloud storage company to use. They evaluate each service for speed, reliability, security, ease of use, cost and tech support. The top 10 programs at that time were **JustCloud.com**, **ZipCloud.com**, **myPCBackup.com**, **SOS.com**, **SugarSync**, **Mozy.com**, **Backupgenie.com**, **Dropbox.com**, **Box.com**, and **CrashPlan.com**.

Fortunately for lawyers, several states have now adopted Ethics rules that generally favor the use of the cloud for client data storage, but all of them impose specific requirements for measuring the reasonableness of the lawyer in deciding to use those services. Even the ABA has responded to this issue by adopting relevant amendments to several of its Model Rules, including Rules 1.1, 1.6, Comment 15 to Rule 1.6, 5.3 and 1.9©. These too generally approve of using the cloud with appropriate cautions.

Cloud storage services such as **Dropbox**, **Google Drive**, and **SugarSync**, while inexpensive, convenient and efficient, are notoriously insecure. Not only are files rarely encrypted, but data transfers are typically not protected, and the compa-

Mr. Hodges is an attorney in Denver, Colorado, and formerly served as Co-Chair of the American Bar Association's Real Property, Probate and Trust Law Section Technology Committee. He currently serves as a member of that Section's Communications Committee and the Technology in the Practice Committee of The American College of Trust and Estate Counsel.

nies are usually able to access your files even if they state they won't. Further, they may be legally compelled to do so (read the Terms of Use Agreements and Disclaimer Policies). Certain documents such as client data or sensitive files need to be protected.

Your solution for these files is to either utilize a special, ultra-secure data encryption provider such as **Wuala**, **Tresorit** or **McAfee Personal Locker**, or use a client-side encryption tool to encrypt the files yourself before uploading them to one of the larger storage services such as Dropbox. Let's now examine some of the leading ultra-secure data encryption providers in more detail.

Wuala

- *Price:* 5GB Free; Plans starting from 20GB for $4/month
- *Platforms:* Windows, Linux, iOS, Android

Wuala (wuala.com) is a secure cloud storage service offered by the storage company LaCie. This service differs from mainstream cloud storage providers in two significant ways.

First, they use client-side encryption for files. This means that all of your files are encrypted locally on your device before being sent to the cloud. This ensures that even on a non-encrypted transfer, no readable data can leak out. This process is more secure than a secure transfer, mainly because it means that nobody except you ever has access to your data.

Second, they use a Zero-knowledge password policy: Only you know your own password, and, therefore, only you can gain access to your account. Wuala's employees cannot see your password, nor can they see your data except in raw form (how many files you have and how much storage space they take up, etc.). So, even if someone from the government came knocking on Wuala's door and asked them to turn over your files, they simply would not be able to do so. Nor will you be able to get to your files if you forget your password, so you need to keep and guard it carefully.

Security aside, Wuala operates pretty much like most of the other cloud storage services we all are used to. Simply download Wuala's application and the service will install a special sync folder to your device, where you can drag and drop files to store both locally and in the cloud. Wuala also offers backup and versioning tools that enable you to access previous versions of files or restore files should you accidentally delete them.

Tresorit

- *Price:* 5GB Free; Plans starting from 100GB for $7/month
- *Platforms:* Windows, Mac OS X, iOS, Android

Tresorit (tresorit.com) is a cloud storage provider that claims to offer a truly secure cloud storage service. Security features include client-side encryption, secure data transfer, and secure data centers that are equipped with physical security measures that guard against intrusions, as well as uninterruptible power and backup systems.

Tresorit lets you secure any folder on your device, not just special ones the service creates. Like Wuala, Tresorit encrypts your data on your local machine to help ensure that your files are protected at all times.

Tresorit also practices a zero-knowledge password policy, which means that nobody in the company can ever access your password or decryption keys. Of course, the drawback of such a policy is that if you forget your password, you're basically out of luck (you'll have to create a new account, and you'll lose all of your data in the cloud).

Tresorit's main difference from Wuala, and other mainstream cloud storage services, is the ability to turn any folder on your device into a secure tresor (vault). This means is that you do not have to drag and drop files into a special sync folder. Instead, you can simply right-click on an existing folder and tresor it. This is especially convenient if you are digitally organized and you'd prefer not to rearrange your files into one sync-able folder.

McAfee Personal Locker

- *Price:* 1GB free with a subscription to McAfee LiveSafe
- *Platforms:* Windows 8, iOS, Android

McAfee Personal Locker (http://download.cnet.com/McAfee-Personal-Locker/3000-2124_4-75921123.html) is a cloud storage vault that you manage via your smartphone or

Windows 8 device. It can store up to 1GB of data for free, which you can access from anywhere, but only after you jump through a series of security hoops.

McAfee Personal Locker uses face and voice recognition along with a PIN to secure data. The app requires voice recognition, biometric data (facial recognition), and a PIN to verify your identity before giving you access to your files. You must do this every single time you use their system, which may be more than the average user can handle. Alternatively, you can choose to set certain files as low priority (you will only have to enter a PIN to access them), but that weakens the security of those files.

While definitely not the sort of service you want to use for everyday cloud storage, Personal Locker would work well for sensitive documents that you may need to access from anywhere, such as financial and banking records or valuable personal data documents, or legal documents, or medical records, or copies of a client's confidential documents.

Admittedly switching between different cloud storage providers can be frustrating, time-consuming, and potentially a bad financial decision, especially when providers such as **Copy** (copy.com) offer 20GB of free storage right off the bat. If you would rather not start from scratch, you can still use client-side encryption to keep your important files safe and secure, while continuing to use your insecure, mainstream cloud storage provider. Free applications such as **TrueCrypt**, for instance, will let you encrypt your files inside your Dropbox folder. You will need to have TrueCrypt installed on any device you want to access the files from. Note that, according to a 6/2/14 article in Forbes by James Lyne, an announcement was posted on the TrueCrypt Web site on May 2, 2014 stating that further development of the program was being abandoned because Microsoft had terminated support for Windows XP and that it was not considered secure and might contain unfixed security issues. This was later changed on May 28th to a warning and a set of migration instructions, including for migrating to Microsoft's BitLocker which operates on the newer versions of Windows. In addition, all older downloadable versions of TrueCrypt were removed in favor of one new Version 7.2 which only allows decryption. Thus, further use of this program should be approached with appropriate cautions. For more information, see http://truecrypt.sourceforge.net. For more tips on encrypting your files, check out the PC World guide on how to encrypt (almost) anything that can be found at www.pcworld.com/article/2025462/how-to-encrypt-almost-anything.html.

Additional Thoughts

While doing research for this article I ran across a few additional handy tidbits of information about cloud computing that I want to pass along. One is an article entitled *"9 Tips to Safely Use the Cloud"* This article can be found on the LTN Law Technology News 4/29/14 Daily Update Web site at www.lawtechnologynews.com. Another is a recent article in the May 15th issue of The Lawyer's PC by Editor Daniel E. Harmon entitled *"The 'Mushrooming' Cloud: We're All in the Cloud Already, Why Not Explore It?"* It indicates that recent statistics show that indeed the use of the cloud by those of us in the legal profession has finally arrived. A third one is in the July 2014 issue of Consumer Reports which contains an article entitled *"Your Secrets Aren't Safe"* that details how data thieves can access your most private information, even when it is stored in the cloud. The fourth one is the 2014 edition of the **Clio Cloud Conference** that is going to be held in Chicago, Illinois on September 22 and 23, 2014, and is offering up a conference agenda on cloud computing issues that rivals the more broad technical agendas of the annual ABA Techshow. Thus, this could be a must-attend event for anyone who is seriously contemplating jumping into the cloud world. The last one is the fact that the **American Bar Association** itself is currently working on developing an ABA-hosted cloud service for its members. One can only hope that a product, developed for lawyers by lawyers, will be as secure if not more secure than the cloud products that are mentioned above.