Lawyers in the Cloud – Can You Trust Online Storage?

By Christopher B. Hopkins

Law firms, like other businesses, suffer from data storage burdens and they struggle with the need to access files remotely. Often lawyers cannot send or receive large email attachments due to size restrictions. Increasingly, the solution rests in third party "cloud" storage providers. It could be a private cloud, where your entire system is hosted online, or a public cloud, such as Dropbox, which helps lawyers send or remotely access a subset of their files. The risk, however, is that cloud storage is an emerging technology with unclear legal and ethical boundaries.

In March 2012, the Fraunhofer Institute reported its study of the security methods of several cloud providers (bit.ly/M0Rvdu). Fraunhofer is likely an unfamiliar name but it is a massive, well-respected German research society which created, among other things, the MP3 file format. Ironically, the study results are limited since (a) they examined only seven cloud providers, (b) there was no clear winner, and (c) any cloud updates after the study changes the results. Instead, the study raises awareness of the points where danger can arise. Here are some initial considerations before you leap into the cloud.

Is the "cloud" inherently dangerous?

Lawyers often think of security in terms of preserving a client's confidentiality. Some lawyers fear that email is unsecure but common business practices have galvanized the acceptance of email. The legal concept of "confidentiality" rests on the notion that third parties have been excluded. Leaving files with a third party requires some steps before confidentiality is achieved. Law firms rely on third party shipping and storage companies in the physical world; simply because we do so in the virtual world should not be cause for blind panic.

Reasonable concern, however, arises from the fact that digital transmission and storage of confidential information involves numerous third parties, known and unknown, as files travel over wifi or cell networks, through ISPs and email services, and across the various intermediary nodes of the internet. Before using a cloud service, lawyers need to ask what security is used during transmission and storage; if you do not understand the terminology, use a Google search to see how the IT community views the proposed security methods. Despite a cavalcade of news stories about hackers, data loss, and downtime, the general consensus is that responsible cloud computing is reasonably secure.

Where is your cloud located?

We call it a "cloud" but your data is stored terrestrially, somewhere. Consideration should be given to whether your data is stored domestically or internationally. If your provider is outside of the U.S., be aware of export laws, application of non-U.S. laws, seizure by foreign governments, and enforcement of your contract rights (to say nothing of slow latency in your internet connection). Inside the U.S., providers are subject to the Patriot Act but you also have Fourth Amendment rights. There are jurisdictional considerations – will the location of your cloud-stored data create a "presence" where you do not want one? Also, what happens if the cloud provider's servers are seized due to the actions of another client? Some redundancies, beyond a single cloud, may be in order. Finally, even with redundancies, make sure that a single natural disaster (e.g., a hurricane in Florida) does not risk both your cloud and your local data.

Trust… but verify

When storing data with a third party, you should consider encrypting your files. First, make sure that the connection between you and the cloud is secure through HTTPS or some other transport layer security. Second, ensure that the cloud stores your files in an encrypted format. Encryption can be done before data is transmitted to the cloud ("client-side" encryption) and/or upon arrival in the cloud ("server-side" encryption). Either way, there is the risk that the client (you) might lose your password or fail to limit access. With server-side encryption, there is the concern that a third party (malicious or not) has access to your data and that you may lose control of once-encrypted data if your provider receives a formal demand for access to your data. To this end, client-side encryption may be preferred.

File sharing risks

Often you need to send a large file via email but your system, or the recepient's, declines a file over a certain size. The workaround is to use a cloud to store the file and then you simply email the file's URL address. Using DropBox, for example, you can open specific files so that others have access.

If your cloud has this service, make sure that the file's URL address does not contain information about you or the filing structure which might betray hints about other data (Fraunhofer recommends that the cloud generate a "unique identifier" in the URL). There should be a time-limit to how long it is accessible and the cloud provider should ensure that the file is not so public that it can be indexed by Google.

Recommendations

Digital file retention requires reasonable precautions and redundancies. For cloud storage: (a) keep a reasonably up-to-date secondary backup in a separate location, (b) consider client-side encryption before your data is sent, and (c) ensure responsible password and access protocols are followed at your firm.

Christopher Hopkins is shareholder at Akerman Senterfitt. Feel free to pierce through the wispy clouds of the node-ridden internet with an unencrypted communiqué to christopher.hopkins@akerman.com.