The Legal Intelligencer

Dropbox and the Impact of Personal Cloud Storage on ESI

We have all heard and read about the ubiquitous Internet "cloud." But what exactly is the cloud? And what specifically does that mean for e-discovery?

David Walton and Rachel Fendell Satinsky

2013-01-29 12:00:00 AM

We have all heard and read about the ubiquitous Internet "cloud." But what exactly is the cloud? And what specifically does that mean for e-discovery?

The cloud is really nothing more than computer space that is accessed via the Internet. So, when someone says that they are "storing data on the cloud," all that really means is — rather than storing their information on their own computer that is in their physical presence — they are renting space on a computer to store their data. This storage is then available from anywhere the user can access the Internet.

Several companies have been using cloud-based solutions for several years. One of the most prominent is salesforce.com, which is an online customer relationship management (CRM) database. Instead of buying software, a computer server and an IT tech to run its CRM database internally, a company can subscribe to salesforce.com, store all of its CRM information on a password-protected database and let specific employees access the database from the road, their offices or their homes — anywhere they have an Internet connection.

Google Docs uses the same concept. Instead of buying software and a computer and paying for tech help, a company can just subscribe to Google Docs, use a Web-based version of Microsoft Word and store all of its information on the cloud. This way, companies save money on software and hardware costs and they don't need to worry about having a tech person on the payroll or on call. All of that is managed by Google at a central location. If you need more space, you can just increase your monthly subscription. It's a very economical and efficient pay-as-you-go model. For this reason, a lot of companies use an enterprise version of Google's Gmail instead of buying an email server and paying for its upkeep. Indeed, the ease and cost-efficiency of cloud-based services inevitably means that the "cloud" will continue to grow.

One type of cloud application is growing particularly fast. The market for cloud storage is booming. Cloud storage is the most basic cloud application. It is literally space on a shared server that is rented to a subscriber. Companies in this business have huge, central server "farms" that store incomprehensible amounts of data for their subscribers. Users can access their data stored on these services from any location where they have an Internet connection. These services also can be accessed from many types of devices including laptop and desktop computers (operating on both Windows and Apple systems), tablets

and smartphones.

Dropbox is probably the most popular form of personal cloud storage. Users can get a free account that can store 2 gigabytes to 18 gigabytes of information (depending on how many referrals the user makes). Because one gigabyte contains approximately 75,000 pages of data, that's a lot of potential documents that can be stored on a free account. Once users run out of free space, they can upgrade their accounts to 100 GB of storage ($99 per year), 200 GB of storage ($199 per year), or 500 GB of storage ($499 per year).

The number of Dropbox users continues to grow exponentially. In April 2011, 25 million users subscribed to Dropbox and saved 200 million files a day. Those numbers increased in May 2012 to 50 million users saving 500 million files a day. And, as of November 2012, Dropbox had more than 100 million registered users across the world storing more than 1 billion files a day. Dropbox's estimated value is $4 billion.

Based on Dropbox's success, several ?competitors have entered the cloud storage market. Microsoft SkyDrive, Apple ?iCloud, Google Drive, Amazon Cloud Drive and Sugar Sync all offer cloud storage services. As such, cloud storage is booming. In 2012, there were about 500 million cloud storage subscriptions globally. By 2017, that number is likely to exceed 1.2 billion subscriptions.

Cloud Storage and E-Discovery

So what does all of this mean for litigators and trial lawyers? If you hated dealing with electronically stored information (ESI) before, cloud storage is not going to make your life easier.

As we all know, once litigation becomes reasonably foreseeable, parties are required to issue a litigation hold notice directing custodians to preserve all potentially relevant data. The notice should be sent to all custodians with potentially relevant data and information. With the increasing use of Dropbox and other cloud storage services, parties must update their litigation hold notices to include cloud storage services as a place where relevant data could be located, specifically listing Dropbox (or other cloud storage) as a possible storage site.

But what happens if the employee, not the employer, started the account? Does the employer still have to preserve information on that account? Most times, the answer is yes. This is an issue of custody and control. Just because the account is personal does not mean that employer can ignore it. In fact, most employees have Dropbox accounts so they can store their employers' information and access it from remote computers, their smartphones and tablets. Because most employers allow this, are on notice of it, benefit from it and can force employees to turn over information stored on these accounts if needed for businesses purposes, most courts will find that an employer has a duty to preserve these cloud accounts. Thus, if there's any doubt, you should make sure that individual employees who store business-related information on their cloud accounts preserve their accounts until it can be determined whether unique and potentially relevant information is stored on the account.

Once discovery starts, parties should be on alert for ways in which Dropbox and other cloud storage devices could impact the discovery process. This may include modifying definitions, document requests and interrogatories in written discovery and adapting questions posed during depositions, particularly during the deposition of an IT custodian or other key witness custodian, to include cloud storage devices.

During the collection phase of the discovery process, custodians should be carefully directed on how relevant data will be collected from Dropbox. When information is collected from Dropbox, it is important to carefully document the chain of custody, just as it is important to do so when collecting data from other electronic sources. As a result, securing the services of a computer forensic team may be the best policy when Dropbox is a significant data source. The computer forensic consultant also could serve as a helpful witness if a party's discovery process is questioned down the road or if specific electronic information becomes a key source of evidence.

Even before the outset of litigation, outside counsel should have an open discussion with their clients about how the client stores electronic data. This conversation should include a discussion about whether the client

uses Dropbox or a similar cloud storage system to store electronic data. Awareness up front about how a client's electronic data is secured, regardless of form, can create a more effective and efficient reaction when litigation arises. It is also critical to understand how a client's data is stored, because employers that use cloud-based storage to store all of their own electronic data can face a host of privacy and ethical issues, as well as significant obstacles in the actual collection of data from the cloud.

Dropbox also has started to have an impact on many types of litigation, but is becoming especially prevalent in patent infringement, white-collar and employee trade secret litigation. Flash drives used to be the tool of choice for employees who wanted to abscond with their employer's confidential information and trade secrets. Now, Dropbox and other cloud storage sites are making flash drives obsolete. The last three trade secret cases I had involved the alleged use of Dropbox to steal information. Apparently, I'm not alone.

Last year, a very prominent case in Pennsylvania focused on a lawyer's use of Dropbox. In February 2012, Elliott Greenleaf sued its former partner and the partner's new law firm for violations of the Computer Fraud and Abuse Act, Pennsylvania's Trade Secrets Act, conversion, breach of fiduciary duty, unfair competition, tortious interference and conspiracy. (See No. 2:12-cv-00674 (E.D. Pa.).) Among other allegations, the complaint alleged that the partner downloaded Dropbox onto Elliott Greenleaf's computers and then downloaded more than 78,000 files, including confidential client information, onto the system before he left the firm. The partner allegedly continued to access the files saved to Dropbox once he joined his new firm. Ultimately, a confidential settlement was reached in the matter.

Similarly, in *Zynga v. Patmore*, No. CGC-12-525099, filed in Superior Court in San Francisco, Zynga alleged that a former employee stored more than 760 Zynga files on Dropbox before the employee left Zynga for a competitor. The complaint further alleged that because the files were stored on Dropbox, the former employee "could (1) retain these Zynga files after leaving Zynga and (2) access them from any computer or mobile device that [the former employee] links to his Dropbox account."

Despite the former employee's alleged attempts to delete his Dropbox account off of his work computer, Zynga still was able to gather "a forensic trail of his wrongful conduct." The court issued a temporary restraining order against the former employee and the case remains pending. In another case, PayPal sued Google in Superior Court in San Jose, Calif., in May 2011, after two senior executives from PayPal defected to Google and allegedly stole PayPal's confidential information and trade secrets on Dropbox.

Thus, parties should ensure that any forensic analyses conducted on electronic devices include investigation for cloud storage programs like Dropbox. A trained computer forensic analyst can search a device for evidence of a Dropbox account and the types of files stored in the account. This type of evidence can be traced even when a user has attempted to delete or cover up a Dropbox account. Often, this evidence must be gathered from the computer itself because Dropbox and its brethren do not generally make it easy to get information from them via a subpoena. These services also generally do not keep deleted information for an extended period of time.

Even when an employee has not intentionally stolen his or her employer's data, an employee still may have stored an employer's data on Dropbox during his or her employment. Employers can help protect themselves from unauthorized use of Dropbox by adopting policies that address where employees may store the employer's data. Specifically, employers should consider amending their confidentiality policies to cover external storage of confidential information. Employers also may consider adopting a policy that permits employees to store the employer's confidential information on a cloud storage service, but also requires that the employee agree to certain safeguards such as notifying the employer about the external storage, agreeing to use a password-protected service and agreeing to return or destroy any employer data at the termination of the employee's employment.

The impact and effect of Dropbox is not likely to diminish anytime soon. Dropbox is becoming increasingly prevalent, particularly because these accounts are easy to secure and can be accessed free of charge. In addition, because tablets and other portable devices that are becoming more widely used are not compatible with USB drives, users have resorted to cloud storage systems like Dropbox. As tablet use increases, so will storage on clouds, and services like Dropbox will continue to gain popularity. As a result,

services like Dropbox are going to start to have a considerable impact on litigation.

It is therefore critical that parties ?and their counsel are well informed about the issues surrounding Dropbox and other cloud storage systems. Even if a party believes that Dropbox is not a relevant issue related to its own electronic data, ?parties and their attorneys still must be informed, because Dropbox accounts ? containing an opposing party's data easily could contain the smoking-gun piece of evidence. •

David Walton *is a member in Cozen O'Connor's labor and employment practice group and co-chair of the firm's e-discovery task force. He concentrates his practice on all aspects of employment litigation. He also assists employers facing challenges posed by information-age technology.*

Rachel Fendell Satinsky *is an associate in the firm's labor and employment group. She represents employers in a wide range of labor and employment matters. She also works with clients to address e-discovery related issues and writes for the firm's E-Discovery Law Review blog.*
