Corporate Counsel Business Journal
July ▪ August 2018
ccbjournal.com

CCBJ

HOW THE CLOUD AND MOBILE DEVICES HAVE CHANGED DISCOVERY

▸ Seyfarth Shaw's Robert Milligan and iDS's Jim Vaughn look at discovery and digital forensics in the age of the cloud.

CCBJ: Why is cloud computing so important in discovery and digital forensics?

Jim Vaughn: Creating and storing data in the cloud is for the most part a cheaper alternative to relying on a company's own infrastructure. It may also be a way to leverage better security, if companies consider the pros and cons of the cloud provider's security compared to their own company's security capabilities. Corporations are embracing the cloud. So I see a growing need for cloud forensics as well as mobile device forensics, which also play a large role in cloud computing and where data can be stored.

With the benefits of the cloud, you are also presented with a set of challenges. For example, if you lack a robust password management system and an employee leaves, they may be leaving with the credentials, which prevents the business from accessing their own data. Another challenge may arise when it comes to investigating an employee's activities around the use of the cloud. Data can be spread across various cloud servers, and collecting that data to support litigations may prove to be very difficult or expensive.

What type of evidence from the cloud and mobile devices can be important during litigation?

Robert Milligan: Documents stored in the cloud or on mobile devices are rich with key evidence, particularly for the type of litigation I specialize in, which is trade secret, noncompete and computer fraud litigation. For instance, if it's a social media profile with LinkedIn or Twitter, profile and associated information can be essential to determinations about whether there has been a violation of a noncompete agreement or a trade secret protection agreement.

With email that is stored in the cloud for individual users, if it is personal email or business email, you will need to understand the framework of how the information is stored and how it can be produced in the litigation. With respect to mobile devices, there's text messaging that exists on the phone itself and information regarding geo-tracking that could be contained on the mobile device, which could be significant, depending on the type of case. In labor and employment cases, certainly, what the employee is doing and where they are when they are doing it can be very material in the litigation.

James D. Vaughn is a managing director in the Costa Mesa, California, office of iDiscovery Solutions. Reach him at jvaughn@idiscoverysolutions.com or at 714-261-0348.

What are some of the technical considerations when retrieving electronic data?

Vaughn: The biggest consideration is how you will connect to the cloud system to collect the data. You may need to collect webmail, cloud corporate email, corporate messaging systems, social media, websites or many other forms of cloud data. Data collection is generally the cheapest part of a litigation, yet it can be the most costly if not done properly. Sometimes you may only get one bite at the apple, and if you have a bad data collection, you may be stuck with that throughout the litigation life cycle.

You should also be aware of metadata that may or may not be available. One example is when a file may have been copied or created on a cloud system. On a typical Windows or Mac computer, that information would be readily available to a forensic examiner. With a cloud-based system, however, you may not be able to obtain that type of metadata. Collecting data might sound simple, and in some cases it may be. But collecting

The biggest consideration is how you will connect to the cloud system to collect the data. While data collection is generally the cheapest part of a litigation, it can be the most costly if not done properly.

from cloud systems can be tricky, and making sure it is done right is critical.

Milligan: You need to have an understanding of the issues around data preservation: how often the data is saved, how often the data is overwritten, how it can be collected, what type of auditing capability there is to assess the evidence, what the retention schedule is and how often things are backed up. When you are conducting litigation, you have to have an understanding of what type of cloud storage you are dealing with. Are you dealing with Google Docs? Are you dealing with Dropbox or SugarSync? There can be differences on material issues as far as how the data is stored and retained.

The same thing is true with respect to mobile devices. Are you dealing with a company mobile phone? Are you dealing with a personal phone that has bring-your-own-device software stored on it? It is a really interesting time, because the evidence is no longer just stored on the company server. It is spread out across the world, and it can be in different locations. You need to understand where all the data is so that you can try to capture as much as you can in a timely manner, and you need to address the applicable laws for the locations where the data is stored.

Certainly, the content contained on these devices or accounts can be useful, depending upon the dispute. Often in these cases, particularly if it is a trade secret, noncompete or computer fraud case, the evidence related to accessing and opening the file, even the fact that the file exists in those devices or accounts, can be very significant.

What are some of the legal challenges when trying to get content from personal devices and accounts?

Milligan: Some of the challenges that come up when you are trying to get discovery are objections that are made on privacy, privilege and proportionality grounds. If you are trying to get emails or text messages and you have pending litigation, you may get objections from the other side about those three issues.

Robert B. Milligan is a partner in the Los Angeles office of Seyfarth Shaw and co-chair of its national Trade Secrets, Computer Fraud & Non-Competes practice group. Reach him at rmilligan@seyfarth.com or at 310-201-1579.

Another issue that comes up in capturing the data is the transitory nature of the data itself. It can be deleted or overwritten just by continuing to use the device, depending upon the specific content or forensic information that might be at issue. Depending upon the needs of the case, if text messages, emails, particular file listings or reports are on a specific device, counsel has to be mindful that they will need to move quickly to have the other side preserve that evidence. If they are not willing to voluntarily turn over the information, then the request gets teed up with the appropriate court to get the information so that it can be used for the case.

One of the legal challenges on that particular issue is that a heightened showing can be necessary in order to get access to some types of those devices. With email, it is expected in litigation that the content itself is going to be discoverable. But when you want to get digital forensic access to particular devices or accounts apart from the content that may be stored there, there is often a heightened showing that is necessary.

There are also concerns about privacy. How is the content on these particular devices or accounts related to the dispute? How do you deal with commingled content that may not be relevant to the case? And assuming that there is relevant information on these devices or accounts, how relevant is it really, particularly in the context of the dispute that is at issue? If we have to decide between 10 different devices and accounts, and all of them may have relevant information, from a cost-benefit perspective, taking into account the value of the case, is it reasonable that all these accounts should be imaged and assessed for discoverable information and produced? Those are some of the considerations that go into getting the content from devices and accounts.

How will cloud computing and digital computing change in the coming years?

Vaughn: Years ago, I saw individuals using the cloud, rather than the collective business world. But then there was a movement by cloud providers to attract corporations by really understanding business needs and showing the value as to how they would reduce infrastructure costs. The ability to instantly share and edit documents and create a well-rounded virtual working environment has converted millions of corporate users to the cloud. I see this trend continuing, and a continued need for data forensics in the future. ■