Bloomberg Law®

Digital Discovery & e-Evidence®

Mobile Device Forensics: Discoverability Across Physical and iCloud Collections

By Matt Witchey and Kevin Leung

As workforces grow increasingly remote, spread across borders in hundreds of locations, corporations are seeking ways to simplify how they collect user data for electronic discovery needs. When a legal or investigative requirement to preserve and collect information from custodians arises, computer forensic investigators typically take the custodians' devices and create a forensic image of them. The device image is searched for key information or evidence such as communications or application data. Today, with most mobile devices being backed up to the cloud (i.e., iPhones that are used for work and are linked to personal iCloud accounts), legal teams are considering new approaches that streamline collection efforts and provide access to device information remotely via cloud backups.

When Bring Your Own Device (BYOD) was first gaining steam, corporations had to consider the rules of ownership and usage for devices that were either owned by the employee and used for work, or owned by the corporation but also used by the employee for personal activity. Now, most organizations have policies in place that define device ownership and user rights to it.

Mobile device management tools that provide IT with controls to ensure compliant usage have become best practice. Among other things, these tools allow a corporation to reset a device's passcode, providing the legal team and investigators with access to it, even in situations where the custodian may not be cooperative.

Where personal cloud accounts are concerned, the question of who owns the data is not as clear. Because many companies allow employees to attach personal accounts to their devices, data ownership sits in a grey area. To access an employee's iCloud backup for an investigation, a corporation would need to obtain the credentials to the account from the employee and would be potentially downloading data from an account that is owned by that employee.

In previous investigations when this circumstance has arisen, we have found that most custodians are cooperative and do provide the credentials to access their iCloud accounts. However, in a situation where the custodian is uncooperative, or the collection involves a citizen of a region with strict data privacy regulations (such as Europe and Asia), it can be difficult to obtain iCloud access. In some cases, there could also be legal implications to requesting or obtaining this type of consent and access.

Matt Witchey and Kevin Leung are computer forensics consultants with FTI Technology. Both are based in New York.

Cloud Backups vs. Forensic Images

With all these factors in mind, it is important to understand the differences between collecting data from an iCloud backup remotely versus taking a full forensic image of the actual device. Legal teams should consider the unique circumstances of each case and weigh these against the expected outcomes of the two collection methods to determine the best way forward. Our team recently conducted tests on these two different options to gain insight into the discoverability of data from iCloud vs. the actual device. Below is an overview of the findings, and the pros and cons we determined from each.

Our team conducted two tests. The first used Elcomsoft, which provides mobile forensic solutions that enable experts to acquire, decrypt locked devices, and access cloud services, to obtain an iCloud image. That image was then loaded into Cellebrite, a leading mobile forensics software that provides digital forensics, triage, and analytics, to parse the data. Those results were compared against a direct image of the actual device created with Cellebrite.

In the second test, we used Oxygen Forensics, another widely used mobile forensics tool, to obtain an image from iCloud; and compared that collection against the device image taken with the same software. In both tests, our team utilized a device running iOS 11.2.

The results of both tests were similar, with the core items such as call logs, contacts, chats, SMS, MMS, and voicemails displaying similarly in all scenarios.

Generally, the differences we found between the device images and the iCloud images were minimal, and based on the types of cases we've seen to date, would not likely present an issue in an investigation. These differences included:

- Some audio files that appeared in the device image were not part of the iCloud image. Specifically, items that were triggered by a ''Hey Siri'' request, which are recorded and stored as WAV files on the physical device but not backed up to iCloud. If a custodian said, ''Hey

 ISSN 1941-3882

Siri, what is the weather in Paris right now?'' the recording of that request would be on the device image but not in the iCloud image. This type of data could be interesting and come into play in an investigation, but would not likely be a key piece of evidence.

■ Photo thumbnails that are used to open a photo reel or for reviewing a thumbnail in an application, and the associated metadata from screenshots, are also not available on the iCloud image.

■ The tests found that some databases and text files did not get backed up to the cloud, due to either corrupt files or there being no data in the files.

■ Application-related plugins—the configurations and plugins for specific apps—are not included in the iCloud backup, but did appear in a forensic image of the device. This could result in a discrepancy between the number of applications found on the physical device collection versus the cloud collection; but actual app activity is synchronized and can be found on the iCloud collection.

■ Passwords to unlock specific accounts are not captured within iCloud but are stored in the device, and therefore some or all of the saved passwords may appear only when imaging the physical device. Again, there may be special circumstances when this would impact the investigation, but in most cases, it wouldn't present an issue one way or the other.

In evaluating these results, we found the following pros and cons for taking an iCloud collection over obtaining a full forensic image of the device:

Pros

■ **Savings**: iCloud collection eliminates travel expenses of sending forensic experts to the device locations for physical imaging; as well time savings for performing the image and for the duration a user is left without a device.

■ **User control**: this option offers a greater sense of security for the device owner, allowing them to perform their own backup and retain possession of their device.

■ **Troubleshooting**: During testing, we looked at the effectiveness of screen sharing software in helping us troubleshoot issues during an iCloud collection. Utilizing software such as Webex or Airplay can allow investigators to assist users with a number of issues that may arise during the backup and iCloud imaging process.

Cons

■ **Security barriers**: As mentioned earlier, it can be tricky to identify who owns the backup data, since iCloud accounts are typically personal accounts, even if the device linked to it is company-owned. To obtain access to an iCloud backup, investigators must have the user's credentials and be prepared to face two-factor authentication. Two-factor authentication is a problem for forensic collection, as much of the software we use is not set up to handle it. In some cases, the user can turn this feature off, but there are times when only the owner of the backup account can gain access, presenting potential obstacles for a cloud collection.

■ **iCloud limitations**: First, not all users have an iCloud account, which of course is required to upload iPhone data to the cloud. Also, many iCloud accounts do not have enough storage to keep everything from the phone and are limited to the baseline five gigabytes offered for free. If a user doesn't have enough storage space, the device will not be backed up. Because the iCloud method requires that the user upload his or her data to the cloud before investigators can download the image, the time for completing the collection can vary and may cause delays in the overall process.

■ **Future uncertainty**: Apple frequently makes changes to its operating systems and the way it handles backups, user security, and other features. Future iOS upgrades may change the way data is backed up in the future, which could impact the options investigators have for accessing iCloud accounts and the type of information that is backed up versus stored solely on the phone.

While our testing has not exhaustively checked every single item that may differ between an iCloud and physical device collection, the findings are encouraging from a discoverability perspective. It appears that generally, the evidence that would be pertinent in most cases is discoverable from both types of collection. Depending on the matter, there may be advantages to using one over the other. For example, a situation may arise in which the legal team needs to easily parse the passwords on a device or view the Siri requests to corroborate other evidence. That scenario could warrant a physical collection. Conversely, a corporation collecting data from 10 different custodians, all in remote locations, would save time and money leveraging the iCloud method.

Given that in most cases the iCloud method is likely to produce the same critical information that a forensic investigator would obtain in person, legal teams now have more options for how they approach collections, and greater flexibility in how they work with investigators to obtain key information. This could be especially useful in matters where a device has been lost or damaged. It is encouraging to know that we can get a complete picture of what someone was doing on his or her device, even if we can't see the device itself and must conduct a remote collection. Still, in high-stakes, 'bet the farm' matters, the surest route is to take images from the device and iCloud and compare evidence across both collections. Ultimately, the decision on which approach to take should be case-specific, and may require consulting with experts to determine the best strategy.

  DDEE ISSN 1941-3882