Legaltech news
SEPTEMBER 2016
An ALM Publication

E-DISCOVERY | MOBILE FORENSICS

FORENSICS TO GO

Mobile device forensic collections provide challenges with current technology.

BY MICHAEL WEIL

ISTOCKPHOTO/ASKOLD ROMANOV

MOBILE DEVICE COMMUNICATIONS and data are increasingly important to litigators, regulators, and investigators. Mobile devices are no longer just phones—they are mobile computers, tablets, text devices and more, with the ability to intentionally or unintentionally contain a record of daily life.

Just as computer data has been critical in litigation matters in the past, data from mobile devices, such as photographs and text messages, can be more valuable than ever before. A complete capture of mobile device data and its backups can provide an essential part of the electronic data collection for a custodian in a litigation or investigation.

Enhanced mobile device security features are designed to protect trade secrets, protect communications or monitor corporate compliance. However, the use of enhanced mobile device security may also impede, or prevent, legitimate access to mobile device data. Further complicating the issue, enterprise data collection tools have not been fully developed to collect mobile device data and communications remotely, and mobile device users employ a

growing number of cloud applications that store data in many locations and formats.

As a result, mobile device data access has become more technically problematic, more time consuming, and more expensive. An organization's security, IT, legal, and compliance teams, therefore, should address the combined effect of these enhanced security features, namely the "mobile cloud," and mobile device forensic collection limitations in their practices and policies.

THE INS AND OUTS OF MOBILE DATA

Mobile device manufacturers layer in encryption, device access controls and other measures that help organizations and users protect and control their data. As recent law enforcement efforts to access data on devices have shown, encryption looms large in accessing data on mobile devices.

ENHANCED MOBILE DEVICE SECURITY MAY IMPEDE, OR PREVENT, LEGITIMATE ACCESS TO MOBILE DEVICE DATA.

A widely-used forensic data collection method involves using device backups as the forensic collection. Some mobile device manufacturers are encrypting backups with a password established by the user during the initial set up of the device. The user must use the backup password to change the encryption password or remove the encryption.

If an individual or organization needs access to the backup data, the user must provide a password to collect the encrypted backup data. This assumes that the user is willing to provide the password. Even if that is the case, however, they still may forget the backup password, which leaves the data collector to obtain an encrypted backup, one that is unusable without the password.

APPLICATION MANAGEMENT

Mobile device data may reside in several locations—cloud applications, email servers, the subscriber identity module (SIM), email servers, cellular carrier records, and on the device itself, to name a few. Cloud applications can be particularly challenging because collectors may not know which cloud applications the user is employing until the they inspect the mobile device. With the increasing expansion of cloud services, the effort to identify and collect cloud-based data from a mobile device can be a time-consuming challenge.

Another vexing, cloud-related issue arises from the many mobile device text and chat applications, particularly those used in regions of the world that have popular applications that are uncommon in the United States. The breadth of mobile device cloud applications, each with their own vagaries, can add time and expense to data identification and forensic collections.

Many organizations have implemented mobile device management (MDM) systems to control and track the thousands of mobile devices in their enterprise. MDMs have the potential to allow legitimate access to items such as text messages and other potentially relevant data stored on the mobile device.

Currently, many MDMs can independently capture short message service (SMS) and multimedia service (MMS) messages, which are transmitted through the telecommunications carriers,

but these MDMs typically lack the ability to capture other text messaging applications.

The MDM limitations, in some instances, are mobile operating system-based—that is, the MDM does not fully interoperate with the particular operating system on the device. In other cases, limitations are application-based—the MDM does not interoperate with the specific application.

Although many enterprises can access their computer assets remotely for data collection, which can reduce burden and cost, there is no solution today that can comprehensively collect mobile device data remotely.

ISSUES WITH PHOTOGRAPHS

The lack of remote forensic data collection capabilities, dynamic mobile cloud user applications, and encryption require time-consuming and disruptive user interviews, often preventing the user from accessing the device during the collection process.

In the case of encrypted backups, forensic practitioners may have to laboriously photograph each mobile device screen to collect relevant data. The photographic time consumption does not end at the point of collection. The photographs must be converted to optical character readers (OCRs) to make the data searchable. With the OCR process, lighting, vibration, device color settings and other photographic settings should be managed carefully to yield usable photos for OCR.

This process takes time, and a custodian may be without their mobile device for days while the photographic collection takes place. Further, the photographic collection only identifies active data, and any data that may have been deleted or rolled off the device will not be available for the matter.

THE FUTURE OF COLLECTIONS

Mobile device adoption and business use is only increasing, and the ability of users to interact with countless applications in their day-to-day jobs and life only compounds the difficulty of collecting and investigating mobile device communications and data. The lack of comprehensive remote data collection capabilities and the current tension between security and legitimate corporate data access further increase the difficulty of addressing mobile device data collection and investigation.

Hopefully, a continued dialog with the mobile device user community and enterprise management can lead to a consensus on the appropriate balance of security and legitimate corporate data access. Until these issues are addressed, and remote data collection capabilities and technologies advance, an organization's security, IT, legal, and compliance teams should address the combined effects of these issues in their practices and policies.

Michael Weil is a managing director and computer forensics leader in the Discovery practice of Deloitte Transactions & Business Analytics LLP.