The Black Mirror in your pocket?

Unique opportunities and challenges associated with mobile devices in investigations and legal matters

The information that the average user sees and interacts with on their mobile phone is only a portion of the vast data their device truly holds. In truth, the data on smartphones is rich and granular enough to build profiles of intimate detail about their users by analyzing their behavior, browsing patterns, whereabouts and much more.
The invention of smartphones has led to a paradigm shift in our everyday lives, both, from personal and business perspectives. This is evidenced by the ever increasing mobile phone usage rate, with some of the Middle Eastern countries such as the UAE and Oman leading the world in mobile penetration rates. The ability to have uncapped information at our fingertips is the epitome of practicality. However, the increased reliance on mobile devices has also dramatically increased the degree to which the data on these devices mirror users’ daily activity.

When it comes to the realm of investigations and legal matters, mobile devices, with their increased magnitude of personal data, can be absolute gold mines. The data found on a mobile device can provide investigators with more pieces of the puzzle, or could provide the smoking gun among these pieces. As with most technological advancements, the opportunities created with these additional sources of information are not without new challenges. This step forward in legal discovery is associated with numerous layers of challenges and considerations that must be addressed in order to make effective use of the data that mobile devices can reveal.

### Pieces of a puzzle

The majority of investigations today involve some form of electronically stored information (ESI). Traditionally, investigations that involve analysis of ESI relied primarily on emails and electronic documents. While these conventional data sources continue to act as rich sources of information in fact-finding exercises, they generally do not provide all the pieces of a puzzle. The integration of the data held on mobile devices can unlock a less abridged story, with a more comprehensive timeline of their custodians’ activities, through combining disparate sources of data such as call logs, messaging applications, GPS coordinates, and many other forms of data either generated by the users, or collected automatically by mobile devices.

Although there is an abundance of cases that include outrageous email communications, people are generally more hesitant to discuss fraudulent activities over business emails while they may be more comfortable having the same conversation through mobile messages, due to the more personal nature of the mobile device. A conventional approach that involves analysis of email data can help identify fraudulent behavior. Adding mobile device data into the same investigation could provide crucial information such as a text message sent or a call placed after an email, and offer additional perspectives through the locations the individual has visited, photos taken or wireless networks connected.

### Understanding the challenges and considerations

#### Legal considerations

The first challenge in utilizing data from mobile devices is whether the companies have the authority to access their employees’ mobile devices. Companies are increasingly allowing or requiring Bring Your Own Device (BYOD) policies due to the financial and logistical benefits. However, organizations should consider the requirements and obligations, both from a legal and technical perspective, when such policies are put in place. Due to the various security, privacy, and legal concerns associated with BYOD, the Sedona Conference published the paper “Commentary on BYOD: Principles and Guidance for Developing Policies and Practices.”

In the event whereby a custodian is uncooperative, there are precautions that the forensic technology specialists need to follow in order to avoid inadvertently wiping the data off a particular device by trying to unlock it with several incorrect attempts.

Meeting Discovery Obligations with the aim of helping companies develop BYOD policies and reducing discovery disputes.

### Access and protecting the gold mine

The next challenge is whether the data on mobile devices is technically accessible, especially considering that the majority of mobile devices are password protected/encrypted. In an ideal data collection scenario, the custodian of each mobile device would provide their passcode or PIN during collection. This may not always be the case as became apparent in the recent court case between Apple and the FBI. The FBI had requested Apple’s help in unlocking an iPhone that belonged to a gunman in the San Bernardino terrorist shooting. Apple objected to providing assistance, arguing that providing assistance in unlocking an iPhone in one instance would give the FBI precedence to unlock every iPhone they encounter, which Apple believed to be an attack on civil liberties. While this case may not always be the case as became apparent in the recent court case between Apple and the FBI. The FBI had requested Apple’s help in unlocking an iPhone that belonged to a gunman in the San Bernardino terrorist shooting. Apple objected to providing assistance, arguing that providing assistance in unlocking an iPhone in one instance would give the FBI precedence to unlock every iPhone they encounter, which Apple believed to be an attack on civil liberties. While this case may not always be the case as became apparent in the recent court case between Apple and the FBI. The FBI had requested Apple’s help in unlocking an iPhone that belonged to a gunman in the San Bernardino terrorist shooting. Apple objected to providing assistance, arguing that providing assistance in unlocking an iPhone in one instance would give the FBI precedence to unlock every iPhone they encounter, which Apple believed to be an attack on civil liberties. While this case may not always be the case as became apparent in the recent court case between Apple and the FBI. The FBI had requested Apple’s help in unlocking an iPhone that belonged to a gunman in the San Bernardino terrorist shooting. Apple objected to providing assistance, arguing that providing assistance in unlocking an iPhone in one instance would give the FBI precedence to unlock every iPhone they encounter, which Apple believed to be an attack on civil liberties. While this case may not always be the case as became apparent in the recent court case between Apple and the FBI. The FBI had requested Apple’s help in unlocking an iPhone that belonged to a gunman in the San Bernardino terrorist shooting. Apple objected to providing assistance, arguing that providing assistance in unlocking an iPhone in one instance would give the FBI precedence to unlock every iPhone they encounter, which Apple believed to be an attack on civil liberties. While this case may not always be the case as became apparent in the recent court case between Apple and the FBI. The FBI had requested Apple’s help in unlocking an iPhone that belonged to a gunman in the San Bernardino terrorist shooting. Apple objected to providing assistance, arguing that providing assistance in unlocking an iPhone in one instance would give the FBI precedence to unlock every iPhone they encounter, which Apple believed to be an attack on civil liberties.
In the event whereby a custodian is uncooperative, there are precautions that the forensic technology specialists need to follow in order to avoid inadvertently wiping the data off a particular device by trying to unlock it with several incorrect attempts. In fact, law enforcement agencies are being trained not to even look at the devices with facial recognition features (e.g. Apple’s Face ID), given that inadvertently failing the facial recognition check multiple times could make the phone request a passcode, or at worst, wipe the data off the device entirely.

While on the subject of data loss, due to mobile devices having a high risk of data spoliation, it is imperative that the secure seizure, transportation and examination of mobile devices are performed by specialists following digital forensic best practices. There are various factors that may impact the integrity of the data collected from mobile devices. For instance, most mobile devices have limited storage capacity, which would sometimes imply an auto-deletion setting being enabled, thereby creating a possibility of data loss. In addition, mobile phones are inherently prone to external interference. Through wireless signals, it is possible to remotely wipe the data off the device or alter the data on the device, which could render the entire evidence item inadmissible in court. When there are risks of external interference, digital forensics specialists would preserve and transport devices with specialist equipment called Faraday bags in order to prevent outside signals reaching the mobile devices.

Cat and mouse – Another challenge associated with data on mobile devices is the processing and analysis of the data. Mobile devices house various third-party applications and different file formats. Processing data from these constantly evolving applications in order to make it available for review purposes is a challenge in itself. Mobile devices house various third-party applications and different file formats. Processing data from these constantly evolving applications in order to make it available for review purposes is a challenge in itself. The electronic discovery industry is constantly trying to keep up with this unparalleled speed and variety of changes.

Finally, there are various challenges with regards to how the data from mobile devices is reviewed and potentially presented in court. One of the challenges is providing disparate sources of information such as call logs, contacts, text messages and chats in a unified and user-friendly method for review. Another challenge is the use of emojis as they are most prevalent in mobile communications. As emojis may contain meaningful content and provide valuable context, they should not be omitted while searching, reviewing or presenting digital evidence. In fact, they are increasingly appearing in court cases.

In summary
With mobile devices acting as mirrors of our daily lives, it is clear that they can provide invaluable information in investigations or legal matters, hitherto unavailable. However, while these devices have the potential to unlock new perspectives in investigations, there are various technical challenges and legal considerations that organizations should be aware of. In order to address these challenges, organizations should be seeking accurate and timely legal advice, and hiring qualified specialists equipped with the right skillset and toolkit to be able to harvest these rich sources of information effectively.

by Nick Athanasi, Partner and Boray Altunisler, Assistant Director, Financial Advisory, Deloitte Middle East

Endnotes
3. USA v. In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGDD203 (February 19, 2016)