Blurred lines

Incorporating mobile devices in corporate investigations

The majority of corporate investigations today involve electronically stored information (ESI). In the past, this has typically amounted to corporate email or computer data.

In this day and age, corporate fraud perpetrators are becoming smarter and more aware of the controls organizations put in place to ensure security and compliance. As a result, fraudsters are regularly circumventing these controls by using both advanced and common personal communication applications and mobile devices to plan, coordinate, and/or execute actions related to fraud and misconduct. Data extracted from mobile devices can be crucial in corporate investigations. However, corporates are urged to have proper controls and mechanisms in place to be able to reap the benefits of this critical information, while still ensuring employee privacy and legal compliance. Failing to do so can result in reputational risk with material consequences.

Importance of mobile devices in corporate investigations

The majority of corporate investigations today involve electronically stored information (ESI). In the past, this has typically amounted to corporate email or computer data, whereas mobile phones were overlooked given the limitations of extracting information of interest in a forensically-sound manner. However, this is quickly changing due to three main factors:

Factor 1: Richness of data that currently can be forensically extracted from mobile devices

The development of mobile forensics, a subset of digital forensics focused on the recovery of mobile digital evidence in a manner that is acceptable by law, and the development of capabilities and functionalities of mobile devices, allow existing forensic tools to extract significant data such as:

- Instant messaging data e.g., WhatsApp, iMessage, Telegram;
- SMS;
- Call history;
- Internet artefacts e.g., history, inputted data;
- Contacts;
- Accounts;
- Multimedia and documents including metadata; and
- System files including activity logs.

Factor 2: High smartphone penetration rates and use in business

With the current smartphone penetration reaching 75% of connections, as well as the significant dependence on mobile devices in people's daily lives, including businesses where 80% of companies believe that mobiles are necessary for employees to perform their jobs, it is very likely to find investigation relevant corporate data on both corporate and personal mobile devices.

Factor 3: Rising flexible work and Bring-Your-Own-Device (BYOD) trends

The rising trend of remote/flexible work and BYOD, as well as a market expected to achieve a compound annual growth rate (CAGR) of 1% over the next 5 years, contributes to blurring the lines between corporate and personal information. These factors make mobile devices, in particular, personal mobile devices, an essential data source for corporate investigations, helping piece together the puzzle or identifying the "smoking gun" in a corporate investigation.

Case examples:

Let's consider WhatsApp as a key mobile data source; it is the number one instant messaging application in the UAE (and probably several other countries), with 80% of the country's population using the application. Whilst some organizations prohibit the use of WhatsApp for business communication within their policies or terms, others welcome it, including governmental entities. In both cases, employees can still use personal or business WhatsApp accounts to plan or commit wrongdoing, leveraging its ease of use, popularity, and end-to-end encryption.

Drawing on the extensive number of corporate investigations we have been involved in, WhatsApp has proved imperative in investigating various types of fraud, such as collusion, conflicts of interest, asset misappropriation, and other forms of misconduct. In one case, a custodian deleted the entirety of the application prior to imaging; however, we were able to prove that WhatsApp had previously been installed based on extracted digital forensic artifacts. In addition, we were able to recover chat data that contained evidence of the custodian exfiltrating confidential data via the application.

Other key mobile data sources include internet browsing history. An organization is likely to monitor web traffic and searches on a corporate-owned computer, but may be less likely to do so (or be able to do so) on a mobile device - particularly personal devices not on their network. In one case, we found that the device owner had searched for anti-forensic tools and techniques in which to delete data on their mobile following a notification of data collection. We were able to correlate this to digital artifacts on their laptop, which indicated the use of anti-forensic tools on the same day. In another corruption case, we were able to recover and correlate web history data related to purchasing expensive gifts for government officials.

Incorporating mobile devices in investigations

Whether a corporate-owned, personally enabled (COPE) or a personal mobile device, special care must be exercised in collecting, processing, and reviewing data from such devices as both are likely to contain personal data. Just like an organization strives to protect its business, it should also ensure it protects its employees' privacy. In most jurisdictions, this is not just a moral obligation; it is also a legal one with severe breach consequences. Personal data collection and processing restrictions will depend on applicable laws. Adequate legal council should be obtained prior to processing such data or implementing related controls.

Key considerations when incorporating mobile devices in investigations include:

Policy considerations

1. Ensure corporate data collection, processing, and transfer policies are in place and conformed to during corporate investigation.

2. Identify restrictions and the legal basis on which personal data can be collected, processed, and transferred.

3. Deploy and enforce personal data processing and retention policies for corporate-owned and BYOD devices.

4. Deploy and enforce policies and guidelines on segregating personal and corporate data.

Policies should include both personal and corporate devices and attention should be on how best to segregate personal and corporate data. For example, with mobiles, the use of two SIMs or the use of WhatsApp Business for corporate matters could help in segregating business and personal communications. In the same way, storage of personal data on corporate devices should be limited and managed appropriately, such as through restricting access or using access logs.

Depending on jurisdiction and policies in place, the organization may have the right to obtain all corporate data, including any business communication on personal devices. However, appropriate legal advice should be sought in all cases. This also includes how data may be transferred, based on the applicable laws and regulations.

Procedural considerations

1. Ensure proper corporate data monitoring, protection controls, and tools are configured, deployed, and monitored as a proactive procedure.

2. Ensure the use of proper forensic tools and procedures within investigations.

3. Obtain adequate legal counsel and explicit consent from the custodian prior to the data collection, processing, and review.

4. Be aware of cultural sensitivities such as gender, religion, and customs, as well as the likelihood that personally identifiable information (PII) will be held on these devices.

5. Consider targeted versus complete data collection approaches.

6. Utilize impartial professional third parties for the collection, processing, and review.

There are various tools available for monitoring activity; for mobiles, at a minimum, Mobile Device Management (MDM) should be in place. More in-depth controls may help detecting and supporting with an incident.

During an investigation, in most cases, custodians are concerned about who will view their data, especially because of the intermingling of personal and corporate data that occurs on mobile devices. We have noticed that custodians often feel more comfortable with an impartial third party holding their data, as opposed to someone from within the organization. A successful approach we have used during several investigations has involved collecting a custodian's data, selecting specific data types to be reviewed, and then performing keyword searching on reviewable data - with only data responsive to investigation defined search terms being reviewed. It is also possible to segregate data collections by targeting specific data sources or applications.

In summary, organizations are strongly urged to be aware of the impact of data privacy laws and regulations when it comes to collecting employees' data for the purpose of an investigation. Whilst data privacy and protection applies to all corporate data sources, mobiles can be particularly complex due to their use in our everyday life and data ownership.

Nonetheless, mobiles and the data they hold often prove critical to an investigation, and end up being the most valuable data source at hand. Implementing the right policies and procedures will help drive an organization's ability to collect and review this data, however, the appropriate controls and considerations need to be in place to ensure the organization respects employee privacy and maintains legal compliance. ●

By **Cezar Serhal,** Assistant Director, **Natalie Forester**, Assistant Manager, and **Faiz Ali Khan**, Associate, Forensic, Deloitte Middle East

Endnotes

[1] https://www.gsma.com/mobileeconomy/wp-content/uploads/2022/02/280222-The-Mobile-Economy-2022.pdf

[2] https://www.oxfordeconomics.com/resource/maximizing-mobile-value/

[3] https://www.mordorintelligence.com/industry-reports/byod-market

[4] https://www.globalmediainsight.com/blog/uae-social-media-statistics/

[5] https://medium.com/damian-radcliffe/how-the-middle-east-uses-whatsapp-6dc921d83d2a