Mobile Forensics: The case for a deeper dive during government and regulatory investigations

Mobile devices have made communication easier and faster than ever by giving people more ways to connect from the convenience of something that can fit in your pocket. They have accelerated the pace of business and widened possibilities by allowing employees greater accessibility to people and information. They allow people to focus more on getting things done and less on administrative and logistical processes attached to using desktop and laptop computers.

As such, there has been an increase in employees using personal mobile devices and third-party communication channels to conduct company business. This creates more risk for the company because it has little control over or access to these business communications. Further, expectations of the government to produce all documents and communications relevant to a request have not changed, and these types of communications and data sources are more commonly being scrutinized during government and regulatory investigations. Additionally, there is now significant government and regulatory focus on “off-platform” or “off-channel” communications, including text messages, instant messages, and communications via third party messaging applications such as WhatsApp or other ephemeral chat services.[1]

> The messaging from regulators surrounding recent significant enforcement actions has made clear that the Enforcement Divisions of the SEC and CFTC are going to continue to probe firms’ recordkeeping relating to employees’ personal devices,” said Kristy Littman, Partner at Willkie Farr & Gallagher LLP. “For registrants with record keeping obligations, proactively reviewing policies and procedures and remediating any deficiencies in anticipation of that increased scrutiny is highly recommended.

Regulatory attention toward off-platform communications

U.S. regulators have taken notice of the prevalence of off-platform communication in their investigations, particularly during the pandemic. They have levied large fines for companies’ failure to monitor their employees’ electronic communications, causing potential breaches of rules that require retention of business records.[2] Further, “under SEC and CFTC rules, brokerage firms are supposed to preserve and monitor their employees’ written communications, which creates a paper trail for regulators who check compliance with investor-protection laws.”[3] The financial service industry is experiencing record fines of approximately $2B as regulators, including the SEC and CFTC, find that off-platform communications unavailable to companies were a hindrance to their investigations.[4]

[1] https://www.sec.gov/news/press-release/2022-174

[2] https://www.sec.gov/news/press-release/2022-174

[3] “Banks Nearing $1 Billion Settlement Over Traders’ Use of Banned Messaging Apps,” by Dave Michaels – *Wall Street Journal*, August 19, 2022.

[4] “Wall Street's Record Fines Over WhatsApp Use Were Years in the Making,” by Stefania Spezzati, Matt Robinson, and Lydia Beyoud – *Bloomberg*, August 16, 2022.

The Department of Justice (DoJ) has also increased focus on this type of activity. In a recently published DoJ memo regarding corporate criminal enforcement policies, the Deputy Attorney General emphasized concern over corporations' usage of personal devices and third-party applications, and the ability of compliance programs to monitor for misconduct and recover relevant data during investigations. In assessing a company's cooperation during a criminal investigation, "…prosecutors should consider whether the corporation has implemented effective policies and procedures governing the use of personal devices and third-party messaging platforms to ensure that business-related electronic data and communications are preserved."[5]

Effect of BYOD policies

Most companies allow employees to purchase and use their own personal devices and service plans for business use, the costs of which are then either partially or fully reimbursed by the company. One of the primary drivers of Bring Your Own Device (BYOD) policies is cost reduction and efficiency for the company. From a risk perspective, the employer has no access to the personal content, nor sufficient control over the personal data on the device, which makes preservation and production of this information very challenging. There are no enterprise level capabilities to search the BYOD mobile devices and retrieve documents and files that may be relevant to an investigation. This means the company and its counsel must rely on individual employees to cooperate with and assist them in the retrieval of potentially relevant information. Until Mobile Device Management (MDM) software has options to access content on these devices, it is critical for the company to have a process for obtaining consent and the ability to individually preserve, search, and produce documents from each device in use.

With the proliferation of mobile devices, use of mobile device applications to conduct business has grown at a rapid pace and use of desktop and laptop computers has declined. In some cases, employees even use mobile devices as their primary mechanism for work communications. Android is reportedly more popular globally, but iPhones and Apple iOS leads the market in the U.S.[6] The Apple iOS changes frequently and is keenly focused on user privacy and data security. In fact, the newest version of Apple iOS has added many new user features that can have an impact on investigations, such as the ability to edit and unsend messages, and recover recently deleted messages. Commercially available forensic software for mobile device analysis cannot keep pace with the changes, making it challenging to have tools available that can access all data on Apple devices during time-sensitive investigations. More importantly, the commercially available forensic software lacks the ability to tell the story of a user's activities.

Mobile forensic complexity

Many forensic practitioners receive training for how to use forensic tools, but do not have a deep understanding of mobile operating systems, how data is stored on mobile devices, and the forensic artifacts available on a device that can help explain user activity with a high level of detail and certainty. Because of this, there is significant risk of overlooking important data and activities related to the matter. This can result in investigators and attorneys missing key evidence that can help inform legal strategy and shape the defense of a client.

[5] https://www.justice.gov/opa/speech/file/1535301/download
[6] "Why is Android more popular globally, while iOS rules the US?" by Jack Wallen - Mobility published by TechRepublic, May 12, 2021."

When it comes to communicating on mobile devices, users have a plethora of application (app) options to choose from. Use of apps can depend on many factors, including popularity of apps in different regions of the world, ease of use on Android versus iOS, device type with which the user is communicating, availability of encryption in the app, and personal preference. Some of the most popular apps include:

1. eMail
2. SMS and/or iMessage app
3. Whats App
4. WeChat
5. Signal
6. FB Messenger
7. SnapChat
8. Telegram
9. LinkedIn
10. Twitter

Before diving into analysis of data from each app, forensic practitioners must understand if the data is stored within the application on the mobile device or in the cloud, and, if it is encrypted, ensure it is properly collected and accessible. For example, Signal data is only stored on the device and is encrypted, so the forensic practitioner should confirm the Signal data is accessible after the collection is completed and before the device is returned to the user. Other apps that store data between the mobile device and the cloud can be impacted by user settings, synchronization issues, and other factors, making documenting the application settings and synchronization status critical for accurate analysis and reporting. The use of rapid reports that contain information such as installed applications, sizes, and last used information can be used to quickly identify potential data sources of interest and verify completeness. Further, these reports allow interviewers to ask questions about potential data sources when custodian interviews and collections are taking place in parallel.

After ensuring completeness of the collections, forensic practitioners must be able to understand information parsed by the forensic tool automatically to help tell the story of user activity. For example, the Recents database on Apple iOS contains information parsed with iMessage chat data but is often overlooked. Metadata such as sender/recipient, contact information, and timestamps of when iMessages were sent/received are available in the Recents database. In certain situations, this metadata will remain after messages are deleted and with close analysis can be used to identify potential evidence of message deletion.

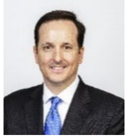
Chat data presents unique challenges in the way it is stored on the mobile device, captured, and exported by forensic tools. Chat threads can span years and be quite voluminous, making it challenging to review. This is especially important when multiple devices are collected, which can further exacerbate the problem. Review can be facilitated by transforming chat data into a reviewer-friendly format that closely resembles the user experience on the mobile device and loading into a review tool to utilize searching/filtering capabilities. Further, unitizing chat conversations into manageable segments is important to assist with quickly locating relevant portions of long conversations and distributing chat conversations among multiple reviewers. When it is time for production, this reviewer-friendly format and unitization is extremely important to providing the data in a format the other side will accept without issue and minimize the amount of time invested in redactions. For example, smaller unitization can help avoid having to redact large portions of long chat threads that are not relevant.

The Way Forward

All these issues, risks, and challenges can make current mobile forensics seem overwhelming. Unfortunately, the government and regulators often have little sympathy for the targets of their investigations in dealing with these challenges. The best course of action is to prepare in advance of an investigation and get the right help as early as possible when you become aware of a new investigation. It is critical to take the time to understand how employees *actually* communicate and not just focus on the mechanisms and tools the company provides. Bring in a forensic firm to help identify where potentially relevant communications might exist, preserve the evidence, and analyze the communications to tell the story of who, what, when, where, why, and how. Determine nuances and identify aggravating and mitigating factors as early as practicable – ideally at the beginning so that counsel can provide the best advice possible. If they don't have the detailed facts, their representation will be handicapped unnecessarily. Those counsel who get this right will be able to focus their legal talent on the merits and actual legal issues, which can only benefit the outcome for the company.

Having a clear understanding of how employees communicate as well as of where and how the data is stored allows counsel to quickly access the relevant materials to analyze early on the strength and weaknesses of a matter" said Olga Greenberg, Partner at Eversheds Sutherland LLP. This approach the best way to minimize surprises later on in the investigation and in litigation.

Contact us



Kenneth C. Koch
Principal, Forensic
(202) 533-7086
kckoch@kpmg.com

Kelly Markgraf
Principal, Forensic
(818) 470-7803
kellymarkgraf@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia

KPMG LLP does not provide legal services.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.