What's the Deal with WhatsApp: Investigating and Discovering Mobile Device Data?

By Julian Sheppard and Michele C.S. Lange

Analyzing data from mobile devices is still uncharted territory for many in Legal and IT. Accordingly, today's modern legal and technology professionals need to brush up on all things mobile. This includes understanding where applicable data resides in a mobile device and what common challenges are associated with accessing, preserving and extracting this data.

To make things complicated, mobile devices contain more than just email, text messages and photos — all fully discoverable in litigation and ripe for investigation. Legal teams cannot forget that inter-application ("app") chat communications may also contain relevant information. Each of these apps store content on the mobile device and function in slightly different manners, creating myriad data preservation, collection and privacy issues.

One such app taking the mobile device world by storm is WhatsApp. This article explores what legal teams need to know about accessing, preserving and extracting mobile data from WhatsApp, in light of recent news and privacy concerns.

The History of WhatsApp

WhatsApp is a stand-alone, cross-platform messaging service for mobile phones. It is marketed as being an inexpensive alternative to carrier-billed text messaging. WhatsApp functions by utilizing a mobile phone's Internet or Wi-Fi connection. Through this connection, the WhatsApp user can send and receive text, pictures, audio or video.

Facebook's Acquisition of WhatsApp

WhatsApp was created in 2009, and since then has made international headlines by becoming one of the most popular standalone messaging platforms. In June 2013, WhatsApp had 250 million users and its user base keeps growing. WhatsApp's popularity attracted the social media giant Facebook, which acquired WhatsApp in February 2014, to play a bigger role in the rapidly growing messaging market. At the time that this deal was announced, WhatsApp had 450 million users worldwide.

The Use of End-to-End Encryption and Its Impact on Privacy

In 2014, WhatsApp implemented end-to-end 256-bit encryption on Android mobile phones, making it possible for secure communications. When a message is sent through WhatsApp, the messages are automatically "locked" once the user sends the message to the receiver. The message will not be "unlocked" until the receiver opens the message. This type of encryption — where the communication from sender to receiver cannot be decrypted during transit, making interception by a "middle man" virtually impossible — makes it unique from other messaging apps.

WhatsApp stresses in a statement from 2014 that not even the best hacker or the WhatsApp company itself can access and read users' messages. In 2016, WhatsApp expanded its end-to-end encryption to other types of mobile phones beyond Android. That same year, WhatsApp decided to make a bold change to its privacy policy by modifying its terms and conditions. Unless the user does not agree to the terms and conditions, users will immediately start sharing their data with Facebook and its affiliated companies, such as Instagram. Shared data will consist of users' phone numbers and the last time they logged onto WhatsApp. The interplay between WhatsApp's end-to-end encryption and these new privacy terms are leaving many users wondering if WhatsApp communications are truly secure and private.

Transitions with WhatsApp's User Base

Despite the change in policy, WhatsApp remains very popular. It is particularly popular in Europe, where unlimited texting mobile plans are less common. Further, WhatsApp is seeking to shift from personal to professional use. Initially designed for personal communications, WhatsApp is trying to acquire a new user base, by having companies adopt the platform, especially if the company has BYOD (bring your own device) or COPE (corporate-owned personally-enabled) policies. Particularly, in some Eastern European countries, WhatsApp has become especially popular for secure business communications because users know it is difficult to access.

WhatsApp Data in Mobile Discovery and Investigations

Drilling into a phone's memory to attain information, such as WhatsApp communications, requires an advanced level of expertise. This is especially true given the intricacy of the phone and the growing ecosystem of device types. Further, mobile device extraction attempts, including attempts to recover data from WhatsApp, typically require phone passwords, PINs (Personal Identification Numbers) or swipe patterns to gain access to the device. Yet, even with this information, and depending on the mobile device itself, if the message data from WhatsApp is encrypted, it may not be possible to extract the data. Thus, even though mobile phone forensics is a fairly new discipline, an investigator needs a firm grasp on both the diversity of devices available on the market and the security measures used specifically on phones if any data is to be forensically retrieved.

Complexity of WhatsApp Mobile Data Extraction

While WhatsApp data may be retrievable from a user's laptop or a cloud account, these possibilities are rare. As such, it is important to understand how the data may be extracted from the mobile device itself. In any forensic investigation of a mobile device, there are factors that influence what and how much data is retrievable. These factors include: the type of mobile device; the operating system version; the version of the specific app being used; and the type of encryption.

When it comes to retrieving WhatsApp communications on mobile devices, all these factors are intertwined. For instance, extracting WhatsApp data is not the same across all devices, as there are a variety of operating systems and versions of WhatsApp. To further complicate matters, WhatsApp's messaging options store content in different locations on different mobile devices and each device functions in a different manner. This lack of standardization is confounding for forensic investigators and case teams involved in the matter. As such, documenting the time and date of the extraction, as well as the operating system and app versions, is critical. Finally, investigators will need the key associated with the local database, which is often inaccessible without special software, in order to decrypt WhatsApp data.

The Debate of the Backdoor and WhatsApp

Currently, there is a major debate among legal and technology professionals about whether or not WhatsApp should have a "backdoor," likely weakening WhatsApp's encryption. When a message is transmitted, a backdoor could be used to circumvent the need for a specific encryption key and convert the message into plain text for it to be read by a third party. Discussed below are the viewpoints of both sides discussing whether there should be a backdoor within WhatsApp.

The Need for a Backdoor

Some security and intelligence agencies prefer WhatsApp to be modified by implementing a backdoor. They argue that this would benefit not only them, but also the public. They claim that

by monitoring WhatsApp messages through the backdoor they can detect criminal and terrorist activity.

One major concern of these agencies is the fear that terrorist organizations will use WhatsApp to communicate with each other, because of the security with end-to-end encryption. As a result of WhatApp's encryption, there has been a recent trend of terrorist organizations using WhatsApp to communicate. In March 2017, a terrorist used WhatsApp moments before carrying out on attack in Westminster, London. This recent attack, and other uses of WhatsApp, has continued to worry these agencies.

Agencies advocate that a backdoor within WhatsApp can have many benefits toward making the public feel more secure. If agencies had access to the messages within WhatsApp, it would give them an advantage to combat criminal activity and terrorist attacks. For example, British Intelligence claimed if they had the ability to read messages communicated by the terrorist back in March 2017, the attack might have been less severe. Thus, if agencies are allowed to monitor messages through WhatsApp, it may help prevent WhatsApp from becoming a safe harbor for terrorist communication.

Weakening End-to-End Encryption

Some security and intelligence agencies believe that modifying WhatsApp by creating a backdoor would be a mistake. Specifically, organizations and individuals will not know in advance whom the government will spy on when they have access to all users' decrypted WhatsApp messages. This could impact how organizations and individuals communicate with each other.

It has been argued that implementing a backdoor will not help, but only weaken WhatsApp's end-to-end encryption. There are other ways that agencies may be able to gain intelligence without the expense of sacrificing security, such as bugging rooms, infiltrating surveillance software, etc. Although having a backdoor is easier, it will sacrifice the security of the end-to-end encryption in WhatsApp and could become a slippery slope to backdoors in other apps.

Lastly, some analysts claim that security and intelligence agencies may have trouble monitoring WhatsApp through the backdoor. Malicious conduct may be hard to detect because of WhatsApp's large user base and the chance of detecting criminal and terrorist activity is minimal. Further, once the public becomes suspicious that backdoors are in place, they are more likely to abandon WhatsApp for a different messaging app that does not have backdoors in place. Thus, by security and intelligence agencies diverting their attention to monitoring WhatsApp, they could lose the public's confidence in the safety net that end-to-end encryption provides.

Conclusion

WhatsApp's controversial end-to-end encryption has affected the ways legal and technology professionals access, preserve and extract this data from mobile devices. Although end-to-end encryption is complex, with help from a seasoned forensics investigator, valuable information on WhatsApp may be just a click, swipe or post beneath your fingertips.

*****

Julian Sheppard (julian.sheppard@krolldiscovery.com) is the Director of Computer Forensics for the EMEA region of KrolLDiscovery, based in London, England. **Michele C.S. Lange, Esq.** (michele.lange@krolldiscovery.com) is the Director of Thought Leadership for KrolLDiscovery, based in Minneapolis, MN. The authors acknowledge the assistance of **Christine Barry**, KrolLDiscovery law clerk for her assistance in researching and writing this article.

—❖—