Report details widespread illegal extraction of smartphone data by US law enforcement

Kevin Reed
16 December 2020

A report published in October by a nonprofit technology rights organization has revealed that thousands of smartphones are searched by law enforcement every day across the US, many of them without a warrant and in violation of the Fourth Amendment's guarantee against unreasonable searches and seizures.

In the report entitled, "Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones," the group Upturn Toward Justice in Technology studied the use of mobile device forensic tools (MDFTs) by law enforcement that enable police to make a complete copy of the contents of a smartphone regardless of its security features.

The extensive and well-documented Upturn report—based on 110 public records requests to state and local police agencies across the country—shows that "more than 2,000 agencies have purchased these tools, in all 50 states and the District of Columbia" and that the agencies "have performed hundreds of thousands of cellphone extractions since 2015, often without a warrant."

The report warns, "Every American is at risk of having their phone forensically searched by law enforcement."

Police agencies use MDFTs to download smartphone data routinely during arrests, both those "involving major harm," as well as those involving "graffiti, shoplifting, marijuana possession, prostitution, vandalism, car crashes, parole violations, petty theft, public intoxication, and the full gamut of drug-related offenses."

The Upturn report reveals that individuals detained by police are often coerced into granting access to their smartphones without realizing the extent of the copying of their personal data and information that then takes place.

MDFTs are powerful tools that extract a full copy of a smartphone's data contents. As the report explains, "By physically connecting a cellphone to a forensic tool, law enforcement can extract, analyze, and present data that's stored on the phone." This includes "all emails, texts, photos, locations, app data, and more."

Upturn reveals that many of the police departments, district attorneys' offices and sheriff departments have purchased the sophisticated phone extraction tools "through a variety of federal grant programs." Meanwhile, departments that have been unable to purchase MDFTs themselves have access to the tools through partnerships and sharing agreements with larger law enforcement agencies and the FBI.

MDFTs have multiple capabilities, such as data extraction, data analysis and security circumvention. Once the entire contents of a smartphone—including contacts, photos, videos, saved passwords, GPS records, phone usage records—have been copied to law enforcement computer systems, law enforcement representatives then set about to use the MDFTs to sift through the data looking for specific information, such as "mapping where someone has been through GPS data, searching specific keywords, and searching images using image classification tools."

They have the ability to circumvent smartphone security features and copy all the data from the device even that which is encrypted. Some of law enforcement extraction tools employ brute-force techniques to guess, for example, an iPhone passcode in "no more than 13 minutes for a 4-digit passcode, 22 hours for 6 digits, and 92 days for 8 digits. The default length prompted by iOS is 6 digits."

In one case, an MDFT developer known as Cellebrite claims in marketing literature that it can "determine locks and perform a full file system extraction of all iPhone devices from iPhone 4S to the latest iPhone 11 / 11 Pro / Max running the latest iOS versions up to the latest 13.4.1." With most advanced MDFT tools, a smartphone passcode can be guessed in under a day.

The Upturn report explains the important fact that not all data on an iPhone is encrypted. They wrote, "certain

data is unencrypted upon startup, including some account information that is needed to receive notifications. For example, Cellebrite's UFED Premium claims it can extract data even on locked iPhones. The data that appears 'before first unlock' (BFU) even includes parts of Apple's password manager. Once the iPhone is unlocked after being powered on—'after first unlock' (AFU)—even more unencrypted data becomes available."

There are other MDFT suppliers, including Oxygen Forensics and Grayshift, that promote their ability to find and extract the unencrypted data on an otherwise encrypted smartphone. In the case of Oxygen Forensics "Detective" software, the tool can extract data "before the first unlock," including image detection that allows law enforcement officials to categorize pictures on an encrypted phone.

The Upturn report does a deep dive into the functionality of the Cellebrite MDFT software and goes step by step through the process deployed by the tool to extract and then analyze smartphone data.

Once a law enforcement investigator plugs the targeted phone into the Cellebrite system, "it will prompt the investigator to choose the kind of extraction to be performed, and, sometimes, the categories and time range of data to be extracted."

Once the extraction is complete, the Cellebrite system moves on to analyze the data and, the Upturn report continues, "law enforcement can sort data by the time and date of its creation, by location, by file or media type, or by source application. They can also search for key terms across the entire phone, just like you might use Google to search the web. This means police can … view them together as a chronological series of events. It also means they can pull all pictures from the phone to view in one place, regardless of how they are organized on the phone."

Other features include functionality that permits law enforcement to retrieve deleted files, as well as data from cloud accounts associated with an individual smartphone. The report says, "an MDFT may be able to pull a remote backup of the phone from Apple's iCloud service by copying information it finds in the phone's password management system and because many services allow users to download all of their data."

The law enforcement tools can also recover log files "showing when applications were installed, used, and deleted, as well as how often someone used an application" and "when a device was locked or unlocked, when a message was viewed, when a Bluetooth device was connected, words added to a user's dictionary, notification contents, as well as past 'spotlight searches' on iPhones, a search function that combines on-device and web results."

The MDFTs also "trace a user's actions on a map or chronological timeline using 'patterns of life' metadata; sort data by file type regardless of its location on the phone … or create network graphs … to infer social relationships using contact data."

In short, the Upturn report has pulled back the curtain on the increasing use by law enforcement agencies of third-party software tools to extract and analyze enormous amounts of information contained on the smartphones of individuals in complete violation of basic constitutional rights.

Cellebrite is an Israeli digital intelligence company founded in 1999. The company came into public view in 2016 when the FBI clashed with Apple over two iPhones recovered from the scene of the San Bernardino mass shooting and attempted bombing. Following the killing of the two shooters by police, the FBI—under the direction of the Obama administration and then FBI Director James Comey—demanded Apple assist in breaking into the iPhones that were found at the scene.

After Apple refused, a public campaign was launched by the US Department of Justice (DoJ) demanding that a law enforcement "back door" be built into the encryption of consumer mobile devices. Later, the FBI and DoJ announced that the iPhones of the San Bernardino shooters had been successfully accessed with the assistance of a third party. Although the FBI has denied it, there were reports at the time that access to the iPhones was made possible through the MDFT services of Cellebrite.