STREET LEVEL SURVEILLANCE

FORENSIC EXTRACTION TOOLS

In today's world, we carry a detailed dossier of our lives around with us. Our mobile devices contain our most intimate details, acting as our private messenger, photo album, scheduler, navigator, address book, notebook, and even wallet all in one. Our devices are a window into our souls. So we are extremely vulnerable when the information these devices contain is accessed by those we don't trust.

Police can use "forensic tools" to extract information from our devices and create a detailed report on our activities and communications.

How Forensic Tools Work

SOURCE: NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

To use forensic tools, police generally need physical access to your device. The first step is to unlock it. Security features in our mobile devices can help thwart such police intrusion, such as an iOS device's Secure Enclave. But these protections have sometimes been defeated by forensic devices. One might view this as an ongoing arms race between the vendors building secure devices for users, versus the vendors building forensic tools for police. So it is important for users to practice surveillance self-defense by, for example, choosing a secure passphrase. Likewise, many users will choose not to unlock their phones when police pressure them to do so.

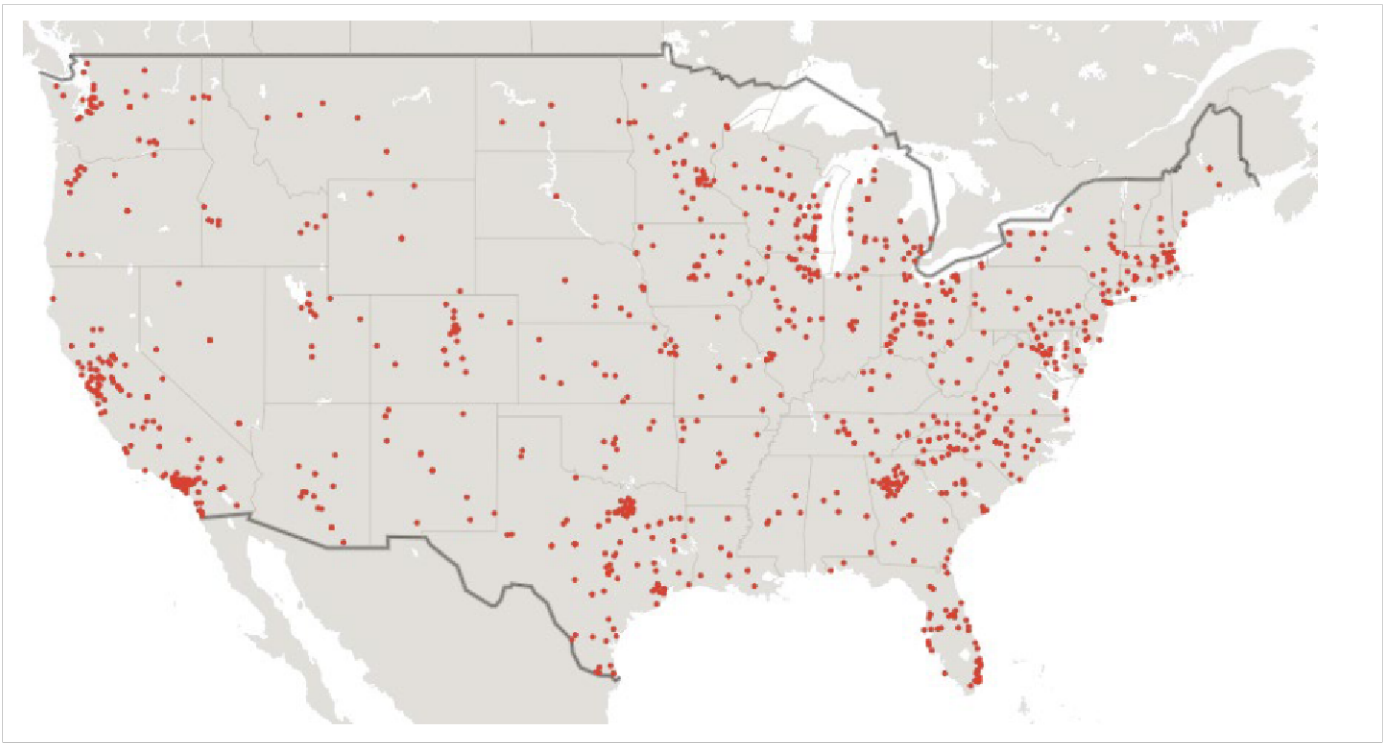
After police plug your device into their forensic tool, they can extract either the entirety of the device contents (sometimes called an "image" of your device), or particular contents such as your entire photo album or a subset of photos. Police might also use a forensic tool to automatically search a user's device for particular types of content, such as all images that contain a unique digital "fingerprint" (sometimes called a "hash").

such as a workstation linked by software. Police can generate reports about a device's content that are easily read and suitable for submission as evidence in court.

What Kinds of Data Forensic Tools Collect

Forensic tools collect a wide swath of information from your devices. This can include photo album pictures and videos, text files, contacts, private and group conversations (even from encrypted messaging apps such as Signal and WhatsApp), any stored location data (e.g. from a map application), events in your calendar, browsing history, and your digital wallets and payment methods. In some cases, an advanced physical extraction of the device can recover content that the user thought they "deleted," but was really still stored on the device.This provides unprecedented access to your private life for anyone willing and able to retrieve this data.

How Law Enforcement Uses Forensic Tools



SOURCE: UPTURN (CC BY)

A map of agencies using mobile forensic extraction devices.

departments, at the border, and even by the US Fish and Wildlife Service. While hacking methods are not uncommon to unlock a phone, police may simply ask you to unlock it in order to gain access. Once unlocked, all bets are off: the contents of your phone can be read by the officer manually, or the device can be plugged into a forensic extraction tool for comprehensive analysis. This is why it is important to make it clear that you do not consent to a search of your device. After all, it is likely to contain the most intimate details of your life!

Once a report is generated of the device contents, police can submit it as evidence in court, or use it to further their investigations. Often it is stored for months or years on a workstation, creating risk of data breach, or misuse by an officer with ill intentions.

Who Sells Forensic Tool Technology

Two major players in the mobile forensic extraction field are Cellebrite and Grayshift. Cellebrite boasts 2,800 customers in North America and some 7,000 worldwide, as of June 2022. Based in Israel, their main line of products is called Cellebrite UFED (Universal Forensics Extraction Device), which is available at various price points depending on what level of extraction is desired.

Grayshift is based in Atlanta, Georgia. Their initial focus was iOS extraction. Since then, they've expanded their business to include Android devices as well. Their main product is known as GrayKey, offered at $15,000 for a 300-use license and $30,000 for an unlimited-use license.

Both of these companies have had their share of vulnerabilities and security breaches. In 2018, hackers leaked segments of the GrayKey code that was left unsecured at a customer site. In 2021, security researcher Moxie Marlinspike demonstrated a security vulnerability in the workstation software accompanying Cellebrite UFED.

The powerful and invasive ability to do forensic imaging of mobile devices is becoming more widespread, and increasingly available to even small police departments and sheriff's offices. It is time to rein this power in.

Threats Posed by Forensic Tools

First, forensic tools are a threat to our privacy. They can vacuum and automatically scrutinize all of the information in our devices.

showing that a user attended a protest, communications between a reporter and their confidential sources, and social media posts on controversial subjects. Widespread police use of forensic tools can chill and deter people from exercising their First Amendment rights.

Third, forensic tools will disparately burden people of color, immigrants, and other vulnerable groups. Police unfairly subject them to a disparately large share of traffic stops and sidewalk stops, and to a disparately large share of searches during those encounters. Forensic tools will be just the newest layer of this discriminatory stack.

Fourth, forensic tools increase the reservoirs of data held by law enforcement agencies, which can be stolen by data thieves and misused by rule-breaking officers.

EFF's Work on Forensic Tools

EFF advocates for new legal limits on so-called "consent" searches. After police use this troubling tactic to coerce people into unlocking their devices, police all-too-often use forensic tools to copy and automatically search the data in these devices.

Suggested Additional Reading

Digital Forensics Unit (Legal Aid Society)

Cellebrite asks cops to keep its phone hacking tech 'hush hush' (Tech Crunch)

TECHNOLOGIES