# We Built a Database of Over 500 iPhones Cops Have Tried to Unlock

17-21 minutes

*With research support from Izzie Ramirez.*

Law enforcement around the country have had varying degrees of success in trying to access evidence from locked iPhones seized from criminal suspects, Motherboard has learned as part of the most comprehensive analysis yet of iPhone search warrants.

Though some law enforcement agencies have accessed evidence on iPhones in the last year, many officials were unable to do so, adding nuance to the debate over whether the Department of Justice should continue its attempts to force Apple to create some form of backdoor in its products that law enforcement agencies could use to more reliably unlock devices.

The analysis found that federal authorities including the FBI, DEA, and DHS have extracted evidence from iPhones in crimes ranging from drug trafficking, to fraud, to child exploitation.

The data adds specifics to the so-called Going Dark debate, a phenomenon where law enforcement agencies say they are unable to access evidence stored on phones or read peoples' encrypted messages even if they have a warrant to do so. Apple and privacy experts say that having encryption enabled on phones and messaging services by default makes everyone safer, and that building a backdoor would make encrypted technology inherently weaker.

In the absence of a backdoor, forensic companies which focus on unlocking or extracting data from iPhones continue to offer their tools, with the price of such tools decreasing dramatically in recent years to tens of thousands of dollars.

"I think efforts like this are important to try to help the public and policy makers understand what is going on," Jim Baker, former general counsel of the FBI and now director of national security and cybersecurity at thinktank the R Street Institute, told Motherboard in a phone call.

Baker was the FBI's head lawyer during the San Bernardino case, where the Department of Justice tried to legally compel Apple to introduce a flaw into a version of its operating system to make it easier for law enforcement to unlock an iPhone. He has since said that public safety officials have to learn to live with encryption because the alternative of introducing a backdoor creates more vulnerabilities in devices that everybody uses.

For all the public bluster on both sides of the Going Dark issue, neither tells the full story. On one side, the Department of Justice has repeatedly advocated for a new method of access, perhaps where Apple would retain encryption keys for devices that law enforcement could then use themselves. When the Department of Justice discusses the issue publicly, they almost never mention that tools do exist which can unlock iPhones in some circumstances, including the latest models. On the other, an overwhelming number of technologists and the tech giants themselves say that creating a backdoor would further expose users to hackers and other threats.

But this debate is most often discussed with anecdotes and not data, and never data that is publicly available, until now. Motherboard collected and analyzed over 500 iPhone search warrants and related

documents filed throughout 2019 to build a database of cases in which law enforcement attempted to get information from an iPhone.

One of the top level findings of Motherboard's dataset is that many law enforcement agencies and officials can not reliably access data stored on iPhones. Whether that's due to a device having too strong a passcode, the phone being damaged, an unlocking capability not being available at that specific point in time, or a particular agency not having access to advanced forensic technology itself, Motherboard found many cases where investigators were not able to extract data from iPhones, at least according to the search warrants.

But in some cases officials were able to obtain data from a variety of devices, including some of the latest models of iPhones offered at the time. Multiple federal agencies and local police departments have access to tools from companies such as Grayshift and Cellebrite, which can, depending on a variety of factors, unlock and obtain data from iPhones.

When state authorities couldn't access an iPhone in a child exploitation case, an official from Homeland Security Investigations, part of Immigrations and Customs Enforcement (ICE), filed for a warrant on their behalf to use more advanced techniques. When a Border Patrol official couldn't get into an iPhone, the agency sent the device to a Regional Computer Forensics Laboratory (RCFL), an FBI-controlled facility with access to phone cracking technology, for extraction.

A screenshot of a section of Motherboard's database. Image: Motherboard

Most of all, the records compiled by Motherboard show that the capability to unlock iPhones is a fluid issue, with an ebb and flow of law enforcement sometimes being able to access devices and others not. The data solidifies that some law enforcement officials do have trouble accessing data stored on iPhones. But ultimately, our findings lead experts to circle back to the fundamental policy question: should law enforcement have guaranteed access to iPhones, with the trade-offs in iPhone security that come with that?

"That there are a number of variables involved here does not sound unique to the context of encrypted devices. Law enforcement does not operate in a perfect world," Riana Pfefferkorn, associate director of surveillance and cybersecurity at the Stanford Center for Internet and Society, told Motherboard in an email. "Entropy happens. Witnesses can be difficult to locate and reluctant to speak to investigators. Memories and bruises fade over time; other physical evidence may be damaged or incomplete. Different agencies have different budgets, and when it comes to digital forensics, they don't all have equal access to specialized personnel and equipment."

"Law enforcement has never been guaranteed that its job will be quick and easy and efficient," she added. "I do not believe law enforcement deserves some guaranteed-reliable means of accessing data on phones."

An FBI spokesperson wrote in an email, "There is a wide disparity of capabilities that exists across the American law enforcement landscape. We must restore and maintain the constitutional balance regarding lawful access to evidence in order to ensure the continued ability of our local and state law enforcement agencies to protect their citizens by investigating local crime and to collect evidence while respecting the privacy of law-abiding citizens. Local, state and federal law enforcement each must be able to exercise their intended mission to protect the American public. Those unique law enforcement jurisdictions should continue to be prescribed by the Constitution, courts and our elected officials, not based upon what a particular industry, company or individual believes is most appropriate." (Lawmakers previously asked FBI Director Christopher Wray to answer questions about the issue, calling the Bureau's Going Dark narrative "highly questionable" after Motherboard revealed that some local police had bought modern iPhone unlocking tools).

Government departments have their own datasets on encrypted devices. FBI Director Christopher Wray repeatedly said that the FBI was unable to gain access to the content of 7,775 devices during the 2017 fiscal year. But *The Washington Post* found the Bureau grossly inflated those statistics, with the correct number being between 1,000 and 2,000. In February *USA Today* reported that the Manhattan District Attorney's Office is unable to access 2,500 devices in its possession. Neither the FBI or Manhattan District Attorney's Office datasets are available to the public.

> ***Do you have access to data on unlocking cellphones? Do you know anything else about it? We'd love to hear from you. Using a non-work phone or computer, you can contact Joseph Cox securely on Signal on+44 20 8133 5190 , Wickr on josephcox, OTR chat on jfcox@jabber.ccc.de, or email joseph.cox@vice.com.***

"This was something that frustrated me tremendously when I was in the government," Baker said. "It was very hard to get good data that we could rely on to make a strong case about how bad the problem was."

Baker said one reason it was difficult to obtain good data was due to how some law enforcement officials don't even bother to go through the process of obtaining a warrant and trying to unlock a phone because they already know that the device is encrypted and they likely won't get any useful information.

"How do you count that?" when there is no search warrant or application available, Baker asked.

To be clear, the data compiled by Motherboard has several limitations that are vital to keep in mind. It does not include every iPhone-related case in 2019: PACER, the court records system Motherboard used to construct the database, is focused on federal warrants, so the data does not include many other cases of local police departments applying for warrants to unlock iPhones that exist. Although Motherboard did create a relatively large dataset, we likely did not obtain every iPhone unlocking case from PACER, due to inconsistencies and variations in how law enforcement officials name such cases, meaning some are filed under obscure titles making them harder to discover.

Sometimes court records can be missing details for no disclosed reason. In some cases, the sheet laying out what specific information investigators obtained was blank or vague. Officials can also make mistakes in their filings. And although in some cases a court docket says the search warrant has been "executed"—that is, acted upon—there is some inconsistency in whether that means whether an investigator was actually able to unlock an iPhone or not. One warrant the ATF executed in an escaped prisoner case said the agency "Attempted forensic examination;" another one the DEA executed said that "Brute force process was attempted." In some cases, suspects provided consent for their device to be searched, but officials sought a warrant in case this consent was later revoked. Law enforcement being locked out of phones is also not limited to Apple's iPhones; law enforcement can have issues with some Android devices as well.

With those caveats, the dataset still presents a snapshot of the Going Dark issue. Out of 516 analyzed cases, 295 were marked as executed. Officials from the FBI, DEA, DHS, Homeland Security and Investigations, the Bureau of Alcohol, Tobacco, Firearms and Explosives were able to extract data from iPhones in investigations ranging from arson, to child exploitation, to drug trafficking. And investigators executed warrants against modern iPhones, not just older models.

A screenshot of a case where investigators were unable to access an iPhone. Image: Screenshot

In some cases, investigators obtained photos, text messages, call records, browsing data, cookies, and location data from seized iPhones. Some executed search warrants explicitly mention the type of extraction performed, such as so-called "Logical" or "Advanced Logical" extraction. The latter is a term with a meaning that varies between different phone data extraction companies, but generally it relates to creating a device backup as iTunes does normally and obtaining some more data on top of that, Vladimir

Katalov, the CEO of iOS forensics firm Elcomsoft, told Motherboard. Katalov said those backups can contain the sorts of pieces of data that investigators obtained, and is available to all models of iPhone.

"The other methods (such as full system extraction) are much more complex to use; they cannot be implemented as [a] 'one button' solution. But return much more data (including conversations in secure messengers such as Telegram, Signal, Wickr etc, not available in backups)," Katalov said.

In one case Motherboard analyzed involving an iPhone, an FBI official wrote they obtained "full extraction," and another from the ATF mentioned the agency obtained "App Data." Obtaining a full system extraction sometimes requires unlocking and jailbreaking, essentially hacking, the device. *Forbes* previously reported on one case where the FBI explicitly said it unlocked an iPhone 11 Pro Max, one of Apple's most recent and secure iPhones at the time of writing, with a GrayKey, the phone cracking product sold by Grayshift.

Apple told Motherboard that the company has responded to over 127,000 requests from U.S. law enforcement agencies over the past 7 years, and that the number of requests has increased over 100%, which Apple says indicates the information the company provides is useful. iPhones often backup certain pieces of data to iCloud, which law enforcement can then access via legal requests to Apple.

In prepared testimony for a December 2019 hearing in front of the Senate Judiciary Committee, Erik Neuenschwander, Apple's director of user privacy, wrote "Given the pace of innovation and the growth of data in recent years, we understand that one of the biggest challenges facing law enforcement is a lack of clear information about what data are available, where they are stored, and how they can be obtained. That is why we publish a comprehensive law enforcement guide that provides this information, and our team has trained law enforcement officers in the United States and around the world on these processes. We will continue to increase our training offerings in the future, including by deploying online training to reach smaller law enforcement departments."

A screenshot of a case where investigators sent iPhones to a specialist FBI lab for data extraction. Image: Screenshot

The current dynamic is that forensic companies find the right vulnerabilities to unlock iPhones, Apple reacts with its own improvements, and then the firms look for other workarounds.

Motherboard previously reported on one flashpoint in the ever-evolving combat between Apple and unlocking firms. In 2018, former Apple engineer Braden Thomas, who went on to work at Grayshift, emailed Grayshift customers warning of an upcoming feature addition to iOS called "USB Restricted Mode." Although the tweak wouldn't defeat the company's GrayKey product entirely, it could mean that law enforcement would need to try and unlock iPhones within a week of them being last unlocked. In future iOS versions Apple made the restrictions on communicating with iPhones over USB stronger too.

Multiple security experts said that Apple will likely make it even harder to unlock its iPhones. That circular dynamic may not be sustainable.

"I think it's going to get harder and harder to find these kinds of unlocking flaws, because Apple does control the entire stack," Alex Stamos, director of the Stanford Internet Observatory and former Facebook chief security officer, told Motherboard. Apple designs and implements everything from the hardware to the operating system itself, which gives it a tighter ecosystem and allows it to push security updates to phones more easily. Android devices, on the other hand, end up having large variations in the security of devices from different manufacturers, which may have their own vulnerabilities or may have difficulty distributing security and Android operating system updates to phones quickly. This means Apple can more easily make sweeping design changes to its phones to thwart any attacks.

A source who works for a company that makes phone hacking tools for governments said that "definitely local access is getting harder due to USB lockdown and similar features." Motherboard granted the

source anonymity to speak more openly about sensitive techniques.

Grayshift's CEO David Miles and Cellebrite's press contact did not respond to a request for comment.

> "It is the world we are in today, and so have to deal with it."

Apple's improvement of the security of its devices is not purely a technical discussion. It leads directly into the DOJ's demands for another approach.

"I think a couple more hardware revisions of understanding the ways that these unlocks are happening and [Apple is] going to make it extremely difficult. Which then will bring this debate back," Stamos said. Rather than relying on cases that have not been wholly persuasive, such as those involving the locked phone of an already dead terrorist, law enforcement may have stronger anecdotes to draw from if iPhones become even harder to unlock, Stamos said. In the latest attempt in January, Attorney General William Barr called on Apple to help unlock two iPhones belonging to a terrorist who attacked a Naval base.

In the December hearing, Senator Lindsey Graham told representatives of tech giants, including Apple's Neuenschwander, "My advice to you is to get on with it, because this time next year, if we haven't found a way that you can live with, we will impose our will on you." (Graham, along with Senator Richard Blumenthal, recently introduced a bill called the EARN IT Act that is designed to combat online child sexual exploitation, but may have ramifications for end-to-end messaging encryption.)

The fundamentals of that debate—what trade-offs is society willing to make around whether officials cannot unlock some iPhones and gather evidence, but every user's general cybersecurity is improved—will likely remain the same.

"Right now, there is no known mechanism to do what DOJ wants to do without introducing substantial cybersecurity risk into the system beyond that which already exists, which is also substantial," Baker, the former FBI general counsel, said. "It makes the cybersecurity posture of the United States even worse." Instead, public safety officials need to rethink not only their approach to encryption, but how they investigate crimes too, Baker added.

"There will be costs in certain types of investigations, but encryption is something that can protect everybody and shouldn't be undermined," Baker said.

He added, "It is the world we are in today, and so have to deal with it."

*You can find the database here, and the related documents here.*