How an iPhone became the FBI's public enemy number one (FAQ)

Sean Hollister and Connie Guglielmo

February 21, 2016

Apple says the fight is about security and privacy for everyone, about the US government trying to compel a public company, using a 227-year-old law, to compromise its most important products, and about setting a "**dangerous precedent**" that would give the US the authority to ask it and other businesses to change their products in the future.

The FBI and the Department of Justice say it's about making sure Americans aren't in jeopardy, about fighting terrorists who are using increasingly sophisticated communications tools, and about a reasonable request to gain evidence from a single iPhone.

Apple CEO Tim Cook says the FBI wants a "master key" that could be used to unlock hundreds of millions of iPhones. The FBI says it's fighting terrorism and that Apple just wants to protect its brand.

Unless Apple CEO Tim Cook gives in or the government backs down, a February 16 court order requiring that Apple build a custom version of its iOS software for the iPhone may turn into one of the most important legal battles over the future of security -- digital security and US national security. Apple has until February 26 to challenge the court's order and says it will fight all the way to the Supreme Court if necessary.

Cook argues the "very freedoms and liberty our government is meant to protect" are at stake. The FBI and Justice Department counter that all Apple cares about is**protecting its business model and brand**.

The fight has raised a lot of questions about what's at stake, which technologies are involved and why complying with the government's request is harder than you might think. We've put this FAQ together to help you get up to speed, and we'll keep updating it with new questions and answers. Feel free to add your questions to the comments section below.

Can you recap how we got here?
On February 16, US Magistrate Sheri Pym ordered Apple to unlock an **iPhone 5C**used by Syed Farook, one of two terrorists who gunned down 14 people at a party in San Bernardino, California, in December. Apple, which was cooperating with the FBI to help the agency access data on Farook's work phone, refused. Cook argues that the order goes too far and that bypassing the password means creating a "backdoor" in its iOS mobile operating system that could be used to access every other iPhone.

Why is this particular iPhone so important to the FBI?
The FBI wants to know who Farook was communicating with and which websites he might have visited in the days leading up to the December 2 massacre. Access to computers and personal phones owned by Farook and his wife would help, but the couple **smashed their personal phones** and removed the hard drive from their computer. Farook's iPhone 5C, given to him by his employers at San Bernardino County in southern California, may be one of their last options.

What's the iPhone 5C?
Introduced in 2013, **it was Apple's lowest-priced iPhone**, starting at $99 on contract. Though it initially came in models with up to 32 gigabytes of storage, Farook had the least expensive model: an 8GB version that was often given away for free with a paid, two-year wireless contract.

Unlike the higher-end **iPhone 5S** announced the same year, the iPhone 5C doesn't include a fingerprint sensor that you can use instead of typing in a passcode.

Apple already gave the FBI data that was backed up from Farook's phone to the company's iCloud online storage service. What's the FBI hoping to find now?
Apple was able to give the FBI backups only through October 19, when Farook apparently stopped backing up the phone. That leaves a one-and-a-half month gap in the data between October 19 and December 2, when the massacre occurred. The FBI believes Farook might have intentionally stopped the automatic backups to hide something.

What's stopping the FBI from just browsing through the phone?
It's locked with a passcode. The FBI doesn't have the code, and neither does Apple. The passcode is stored only on the device itself. Because of Apple's built-in security, you have up to 10 tries to enter a passcode. After that, the iPhone wipes itself -- that is, removes all the data stored on the device.

Why can't the FBI just pop out the memory card or hard drive, or use the fingerprint scanner to unlock the phone?
The iPhone 5C doesn't have any of those things. Data is stored on a memory chip that's soldered to the phone's motherboard. And the iPhone 5C doesn't have a fingerprint sensor.

Can't the FBI use a supercomputer to crack the password or get data off the memory chip?
It's not that simple. iPhones running 2014's **iOS 8** software or the newer **iOS 9**protect their data using 256-bit AES encryption. That's the same standard that protects US government computers against brute-force attacks intended to crack into a device. It could take years to recover data by attacking the iPhone's memory chip, Stratechery's Ben Thompson **explains**.

It's important to note, adds Thompson, that "Apple is not being asked to break the encryption on the iPhone in question...but rather to disable the functionality that wipes the memory when multiple wrong passcodes are entered in a row."

What is encryption? Did Apple create 256-bit AES encryption?
Encryption simply means that information isn't stored in a way that people or computer programs can easily read. It's in code, and to decode it, you need a decryption key. AES, short for Advanced Encryption Standard, is a particularly robust form of encryption that the US government recommends companies use, and one that's been broadly adopted worldwide **since it was introduced** by the National Institute of Standards and Technology (NIST) in 2002.

Why can't the FBI crack the passcode on the iPhone?
Farook's iPhone was set to automatically erase itself after 10 wrong passcodes were entered in a row. That's a commonly enabled feature on work-issued phones.

Even if the FBI could disable the auto-wipe function, breaking the passcode could take a long time -- a very long time. The iPhone requires a minimum delay of 80 milliseconds between each passcode entry, and wrong entries can extend the delay by minutes at a time. Assuming Farook

used a six-digit passcode, Apple estimates it could take 5.5 years to guess. But he might have used a custom combination of letters and numbers. We could die of old age waiting for that.

Besides, there's also the issue of connecting the supercomputer to the iPhone. A unique key built into the iPhone means you can enter passcodes only on the phone itself.

What exactly does the FBI want Apple to do?
The court order asks Apple to create a new, custom version of iOS that runs only on this specific iPhone and that makes three changes to the software. The first two changes would bypass or disable the auto-wipe function and the delay that limits how quickly new passcodes can be entered. The court also asks Apple to add a way to attach a cable or wirelessly connect to the iPhone so the FBI can automatically enter passcodes. That way, the FBI can use a supercomputer to bombard the phone with passcode guesses until it finds the right one.

Is it even possible for Apple to comply with the order?
Security consultant Dan Guido **thinks so**. But that's not the point, says Apple's CEO. Cook argues that Apple can't just bypass those protections for a single phone and expect other phones to stay safe and secure. "Once created, the technique could be used over and over again, on any number of devices," **Cook wrote in an open letter to customers** earlier this week. "In the physical world, it would be the equivalent of a master key, capable of opening hundreds of millions of locks."

Even if Apple did produce a version of iOS that could be used only with Farook's phone, it might be easy for bad actors, like malicious hackers and governments, to use or rewrite that code for other phones, senior Apple executives told us Friday.

If only the FBI and Apple have access to the custom version of iOS, how can bad actors get it?
Senior Apple executives believe that if Apple made a "master key" for the iPhone, it would be an irresistible prize for hackers, and that its own servers would inevitably be hacked. They referenced a joke often attributed to former Cisco CEO John Chambers: "There are two types of companies: those that have been hacked, and those who don't know they have been hacked."

Apple also worries that employees inside law enforcement, or inside Apple itself, could steal the technology.

Could the software be used on newer iPhones, which have added security features?
According to Apple, yes. Though all iPhones newer than the iPhone 5C (and the iPhone 5S) have a protection called the Secure Enclave, senior Apple executives told us the Secure Enclave could be disabled or bypassed using a custom version of iOS.

Apple's also worried that it will create a precedent if it complies with the government's request, that the government might ask it to defeat any security feature that keeps law enforcement from accessing a newer model of iPhone. If you give a mouse a cookie...

Hasn't Apple complied with requests to unlock phones before?
Apple did help law enforcement officials **by allowing them to bypass the lockscreen** -- as long as there was a valid subpoena or a search warrant. It had data extraction technology that let the company's engineers bypass a user's passcode and pull information like contacts, calls and messages. And it did so without having to unlock the phone.

But the release of iOS 8 in 2014 changed that. The new software came encrypted by default, which means Apple no longer had the ability to extract data "because the files to be extracted are protected by an encryption key that is tied to the user's passcode, which Apple does not possess," the company wrote in a **privacy statement on its website**.

The bottom line is that to decrypt the data from Farook's iPhone 5C, you'd need his passcode.

Does the court order let Apple look for another way to get the info the FBI wants?
Yes, it specifically lets Apple find "an alternate technological means" to help the FBI break into the phone. But that alternative doesn't have much wiggle room. It still requires that Apple disable the auto-wipe and passcode delay and create the ability for the FBI to remotely enter passcodes into the phone. Apple believes introducing those security weaknesses could jeopardize other iPhones as well.

Apple had another possible solution: If the FBI placed Farook's phone near a known Wi-Fi network (like the one at his home or his workplace), it might automatically create a new iCloud backup with the missing information. **That idea was foiled** when the county, acting at the direction of the FBI, reset Farook's iCloud password. Senior Apple executives said Friday that was their best idea for helping the FBI get what it wanted. But now we'll never know if it could have worked.

Over the weekend, the FBI released a statement saying that having access to Farook's iCloud account isn't enough. "We know that direct data extraction from an iOS device often provides more data than an iCloud backup contains," **the FBI said**. "Even if the password had not been changed and Apple could have turned on the auto-backup and loaded it to the cloud, there might be information on the phone that would not be accessible without Apple's assistance."

Apple and the FBI also discussed checking to see if the iPhone was backed up to any other computers, and looking over Verizon call records to see who else Farook might have called. But the government determined Farook's phone hadn't been synced with other computers, and the FBI wanted more data than the carrier's call logs could provide. (This is detailed in footnote 7, page 18, of the DOJ's filing on Friday, which we've posted **here**.)

What kind of data could the FBI get from Farook's iPhone if it defeats the passcode?
The FBI should be able to access Farook's text messages, iMessages, photos, videos, contact list and call history, plus any audio recordings he might have made. That's the type of data that Apple has agreed to help law enforcement recover (**PDF**).

Separately, the FBI may be able to see if Farook had any additional email accounts or social-networking accounts. Then the government would have to subpoena the relevant companies for that data.

Why did Apple turn on encryption in the first place?
There are several theories. The New York Times **suggests** that Cook personally believes it's part of his civic duty to do the right thing by customers where privacy is involved.

The same New York Times report says Apple was growing tired of complying with law enforcement requests to hack into its own phones, and decided encryption would "put the keys squarely in the hands of the customer, not the company."

There's also money at stake. After Edward Snowden revealed the extent of government surveillance in 2013, many tech companies were under pressure to show customers that they hadn't been selling their data to the government. As sociology professor Kieran Healy **notes**, Apple is in a strong position to do that, because the primary thing Apple sells is hardware -- not information. That might get people to buy phones from Apple instead of the competition.

What's the 227-year-old law the government is relying on in its case?
It's using the All Writs Act, which was signed into law by President George Washington in 1789, to get Apple to change its software. The act helped establish the judiciary system in the US, giving federal courts the power to issue orders, which were known as "writs" at the time.

Though the law was drafted with quill pens, it's been used in recent times. In analyzing the current standoff, lawyers and commentators often cite **a 1977 case** in which law enforcement asked for the help of the New York Telephone Company to monitor phone calls made by suspected gamblers. **The Supreme Court ruled for law enforcement** in that case.

Over time, use of the All Writs Act has been more or less limited to situations where no other law, statute or provision can be applied, usually because it's extraordinary. As Popular Mechanics **notes** in an explainer, "the shooter's iPhone passcode is certainly an extraordinary situation, which explains why a law from 1789 is at play in a case about smartphones."

Some also believe the government has been waiting for the right opportunity to force Apple to give it access to iPhone data. "The law operates on precedent, so the fundamental question here isn't whether the FBI gets access to this particular phone," Julian Sanchez, a surveillance law expert at the libertarian-leaning Cato Institute in Washington, DC, **told** The Guardian earlier this

week. "It's whether a catch-all law from 1789 can be used to effectively conscript technology companies into producing hacking tools and spyware for the government."

Where can I read the court order and the DOJ's 40-page request for myself?
We've posted those documents in two stories. You can find the three-page court order **here** and the DOJ's February 16 request **here**.

What's next?
Apple had five business days from February 16 to challenge the court's order, but it asked for a three-day extension. Now it has until February 26 to file. Magistrate Pym has scheduled a hearing for March 22 in U.S. District Court for the Central District of California in Riverside. As you'd expect, there will be a lot of legal back and forth, and the case could go through the federal court system all the way up to the US Supreme Court. It's up to Apple and the government to decide how far to take thing, but Apple said it will pursue the case as far as it needs to go, because it's not backing down.