Vox

Apple's battle with the FBI over iPhone security, explained

Timothy B. Lee

February 17, 2016

The FBI captured the iPhone of dead San Bernardino terrorism suspect Syed Rizwan Farook back in December, but encryption technology prevents them from accessing its contents. On Tuesday, a federal magistrate judge in California ordered Apple to write a custom version of the iPhone software that disables key security features and install it on Farook's iPhone in order to foil the encryption.

On Wednesday morning, Apple CEO Tim Cook came out swinging in response. In his open letter to customers, Cook described the FBI's actions as an "unprecedented step which threatens the security of our customers."

"The government suggests this tool could only be used once, on one phone," Cook wrote. "But that’s simply not true. Once created, the technique could be used over and over again, on any number of devices."

While no one is too worried about the privacy rights of a dead terrorism suspect, both Apple and civil liberties groups see this case as an opening blow in a much larger government effort to undermine the security of their customers' smartphone data. Law enforcement and intelligence figures have been arguing for some time now that smartphone encryption is making it harder for them to do their job, while technology companies argue that complying with law enforcement requests will make it impossible for them to protect their customers.

But in this specific case, the FBI is asking for much less than a general back door into encrypted iPhones, and the Bureau argues there's ample precedent for its request. The police have long asked telephone companies, banks, landlords, and other businesses to help them spy on the activities of criminal suspects. As long as the requests are narrowly targeted and receive proper judicial oversight, they have not been especially controversial. The FBI argues that by asking Apple to help them hack into Farook's iPhone, it's just exercising the same kind of power in the digital realm that it's long exercised in other areas of life.

We can expect Apple to challenge the magistrate judge's order. The case's ultimate significance may depend less on whether Apple wins or loses than on the precedent that's set in the process. Giving law enforcement agencies broad power to order technology companies to hack into their customers' devices could be terrifying. But the courts may be able to find a legal principle that allows access in compelling cases like this one without making device hacking a routine law enforcement tool.

The FBI wants Apple to help guess Farook's passcode

The encryption chip on the iPhone uses a powerful algorithm called AES to protect customer data. Each iPhone has a unique number called an encryption key that is needed to scramble or unscramble the data on the iPhone. This key is 256 bits long — that is, a string of 256 1s and 0s — which means there a trillion trillion trillion trillion trillion trillion possible values for an iPhone's encryption key. So if you wanted to crack the iPhone's encryption by "brute force" — guessing each possible encryption key in sequence until you find the right one — it would take many lifetimes even if every computer on the planet were working on the problem.

Apple has chosen not to keep copies of iPhone keys after the smartphones leave its factories. So if law enforcement made a copy of the data stored on an iPhone and brought it to Apple for help unscrambling it, it would be literally impossible for Apple to help.

So then why are we having a debate at all? The reason is that the weakest link in the iPhone's security isn't the encryption itself, but the passcode the user uses to unlock the iPhone. The encryption chip on the iPhone refuses to function until the correct passcode is entered. And by default, the passcode on an iPhone is only four or six digits long.

So while the iPhone's internal encryption chip uses a key with a trillion trillion trillion trillion trillion trillion possible values, the passcode to unlock that encryption chip only has 10,000 or 1 million possible values on most iPhones (if you're extra paranoid, you can enable alphanumeric passcodes, which have many more possible values). So if you're trying to crack iPhone encryption, it's a lot faster to try to guess the user's passcode than the underlying encryption key.

People have built robots to use "brute force" on smartphone passcodes — punching in each of the 10,000 or 1 million possible values one at a time until they find the correct value. A million seconds is only about 11 days, so it doesn't take that long for a robot like this to try every possible passcode.

Apple has added two features to the iPhone to help defeat the attack. First, if the user guesses a password wrong several times, the iPhone will introduce a delay of up to an hour before it will accept additional guesses. Second, the user can optionally enable a self-destruct feature that will permanently disable access to the encrypted data by deleting information needed to unscramble it.

And this is where the FBI has sought Apple's help. The FBI isn't asking Apple to directly unscramble the data on the iPhone — something Apple couldn't do if it wanted to. Rather, the FBI is demanding that Apple modify the software on Farook's iPhone to make it easier for the FBI to guess his passcode. The FBI wants Apple to disable delays between passcode guesses, disable the self-destruct feature, and allow passcodes to be entered electronically over a wifi network or using the iPhone's lightning port. Taken together, these measures will allow the FBI to guess Farook's passcode much more quickly than it could have otherwise — and without worrying about triggering the phone's auto-wipe function.

Apple is worried about a much bigger picture

If this were simply about Farook's phone and the hassle involved in helping the FBI pry it open, it's unlikely Apple would be taking such a big public stand. The concern is that the government is trying to take advantage of a particularly odious defendant to set a precedent that could have much broader implications.

For starters, although the hassle involved in complying with the FBI's request is considerable, once Apple engineers have done the necessary work of creating the custom software it will be much easier to comply with other law enforcement requests for the same service. Today's extraordinary request for an extraordinary suspect, in other words, could be tomorrow's routine request.

And the Farook case comes against the backdrop of a larger debate about whether technology companies should be compelled *in general* to provide government "back doors" into their products. Throughout the past year, FBI Director James Comey has been warning that smartphone encryption is hampering law enforcement efforts. He wants to compel technology companies to provide law enforcement with access to their customers' data on demand. On the campaign trail, Hillary Clinton has called for the technology sector to embark on a "Manhattan-like project" to figure out a way to provide back doors to law enforcement without compromising device security more broadly.

Technologists say that if technology companies deliberately weaken their encryption products to accommodate the US government, they'll simultaneously make those products more vulnerable to hackers and foreign governments seeking to exploit those same weaknesses. Either you build data security systems from the ground up to be unbreakable, in which case the government can't crack them either, or else you deliberately create exploitable security holes, in which case a whole range of bad actors can exploit them.

Apple has tried to tie the debate over the San Bernardino request to this larger debate over back doors, arguing that it shouldn't be forced to provide law enforcement with a back door into its products. But a crucial difference here is that Apple isn't being asked to proactively introduce a security vulnerability into every iPhone. Rather, it's being asked to help hack into the phone of a dead terrorism suspect.

The FBI, having heard the concerns of technology companies, has asked Apple to make custom software that is tied specifically to the device ID of Farook's iPhone.

Civil liberties groups are worried about setting a bad precedent

By itself, it's hard to see the harm in Apple helping the government access the iPhone of a dead suspected terrorist. But Apple and civil liberties groups argue that approving the FBI's request would open the door to more problematic requests in the future.

In the San Bernardino case, the FBI is seeking access to data on an iPhone that's already in its possession. But Julian Sanchez, a civil liberties expert at the Cato Institute, argues that we shouldn't expect the government's requests to stop there. It would be even more useful for law enforcement if they could get Apple to use its software update functionality to install software on phones not in its possession. For example, the Drug Enforcement Agency could ask Apple to install software on a suspected drug kingpin's phone to record all his conversations and send the audio back to DEA headquarters.

Still, much depends on the details of the precedent that gets set in this case. Part of the FBI's argument is that because the iPhone is programmed to only accept software updates from Apple, getting Apple to write custom software is the only way for law enforcement to get access to the data on Farook's iPhone.

That argument might not work as well in the kinds of cases Sanchez cites: Hacking into a drug kingpin's iPhone might be a particularly convenient way to spy on him, but there are likely other ways to spy on drug dealers that don't involve forcing Apple to help spy on its customers. Courts might tell the DEA to use those other approaches instead.

Another worry, Sanchez says, is that if Apple develops software to help the US government bypass iPhone encryption, foreign governments are sure to take notice. And countries like China and Russia have a much more expansive idea of what constitutes a crime.

The FBI says there's ample precedent for its request

The FBI argues that the federal government has long had the power to ask private businesses to help it execute search warrants. Law enforcement groups have routinely asked telephone companies to help it tap suspects' phone conversations, but that's not all. The FBI also pointed to cases where landlords and credit card companies, among others, have been compelled to help the FBI spy on their customers.

And the FBI argues that it's not unprecedented to ask companies to write software in order to comply with a legal request. "Providers of electronic communications services and remote computing services are sometimes required to write code in order to gather information in response to subpoenas and other process," the bureau notes.

Finally, the FBI notes, only Apple can aid the FBI here. The iPhone is designed to only accept software updates from Apple. That means that even if the FBI were able to create its own hacked iPhone software, it wouldn't be able to install the software on Farook's iPhone without Apple's assistance.

New iPhones might not be hackable

One reason Apple is now butting heads with the FBI is that ever since the 2013 revelations of Edward Snowden, the Cupertino smartphone company has been taking stronger and stronger technical measures to resist government surveillance. A couple of years ago, Apple made strong encryption a default setting for iPhones and chose not to retain the encryption keys that would allow it to easily break into the phones at law enforcement's request. Apple hoped that by tying its own hands, it would be able to truthfully tell law enforcement that it was simply impossible to comply with warrants seeking the contents of encrypted iPhones.

But as we've seen, the security measures on the iPhone 5C, Farook's model of iPhone, aren't quite unbreakable, because Apple is still able to install a new version of the iPhone's software to override the protections against password guessing.

But the iPhone 5C is now more than two years old, and Apple hasn't been standing still. The latest iPhone model has a new feature called Secure Enclave that's designed to make the kind of attack the FBI is seeking more difficult.

"The Secure Enclave is a separate computer inside the iPhone that brokers access to encryption keys," security expert Dan Guido writes. "The Secure Enclave keeps its own counter of incorrect passcode attempts and gets slower and slower at responding with each failed attempt, all the way up to 1 hour between requests. There is nothing that iOS can do about the Secure Enclave."

No one outside of Apple knows if the latest iPhone models are truly unbreakable. But in principle, there's no reason Apple couldn't build an iPhone that even it doesn't know how to unlock without the passcode. And there's no law against building such a device.

So if the FBI gets its way, the arms race between law enforcement and technology companies will only continue. Apple is clearly betting that whatever its stance might be, standing up for its own customers' privacy will be a hit in the marketplace.