The Alternative Daily

Tim Cook And Apple Are Fighting The FBI (And For Your Rights)

Megan Winkler

February 23, 2016

There's a fine line that separates safety and freedom, and it's a line our government dances along on a daily basis. Sometimes it threatens to cross it. Such is the case with the FBI's recent request to Apple, which threatens to set a precedent for unconstitutional privacy violations and opens private citizens up to identity theft and censorship. Luckily for freedom-loving Americans, Apple CEO Tim Cook said no.

On December 2, 2015, Syed Rizwan Farook and Tashfeen Malik killed 14 and seriously injured 22 people in San Bernardino, California, before they were killed in a shootout with police. Now Farook's iPhone 5c is in the FBI's possession, and they want full access to it. Investigators say that the phone may contain information that they need to ensure our safety, including the contact information of other terrorists and information about future attacks. Unfortunately for them, the phone is inaccessible as it is currently locked with a PIN code, a four-digit number that locks the phone's screen.

On the surface, the situation seems reasonable: The FBI wants to gain access to one device to find out if there is sensitive information about criminal actions contained behind the phone's security features. But that's not what the FBI and U.S. Department of Justice (DOJ) have requested.

As Roberto Baldwin of Engadget reports, the DOJ wants to be able to access the information in the phone without destroying the encrypted data on the device. More specifically, the DOJ wants Apple to create firmware that would bypass all of the security features on Farook's device. The proposed firmware would disable the security feature on the phone that erases files and data after 10 failed attempts at inputting the device's PIN. Doing so would also "allow authorities to connect the phone to a computer to 'brute force' the passcode so that officials don't have to tap it into the phone by hand."

The problem is, that's venturing into territory so dangerous that Tim Cook, the CEO of Apple, has refused to cooperate with the FBI, despite a court order.

In an open letter to consumers this month, Cook said that the FBI has "asked us to build a backdoor to the iPhone." He continues by writing that "the FBI wants us to make a new version of the iPhone operating system, circumventing several important security features, and install it on an iPhone recovered during the investigation."

Such software doesn't currently exist, and there's a reason for that: Encryption is the one thing that stands between the bad guys and the rest of us. And as it turns out, sometimes those bad guys are investigators within our own government.

The FBI claims that the firmware would only be used once, on Farook's phone. But what would stop the government, which has a history of spying on anyone deemed a "threat" to national security, from doing the same thing to any of our devices? Better yet, what would stop criminals from using the same firmware to access private data including email communications, banking activities and more?

Nothing.

As Cook said, "In the physical world, [the firmware] would be the equivalent of a master key, capable of opening hundreds of millions of locks — from restaurants and banks to stores and homes."

And, as *The Guardian* reports, the FBI and DOJ's battle with Apple has been in the works for a long time. While Apple is working to set a precedent for digital security and privacy, the government is working on setting its own precedent and going to great lengths to do so. In fact, the government is citing a law that's more than 200 years old as justification for its pressure on Silicon Valley.

"The fundamental question here isn't whether the FBI gets access to this particular phone," Julian Sanchez, a member of the Cato Institute in Washington and a legal expert, told *The Guardian*. "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."

The law, the All Writs Act of 1789, is a product of the very first session of the U.S. Congress, and the straightforward law is pretty concise, all things considered:

"The Supreme Court and all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law."

NPR reporter Laura Sydell investigated the precedence for the writ — a fancy way of saying "legal order" — being used with regard to privacy and data security. She interviewed a number of experts, including John Jay College of Criminal Justice Professor Adam Scott Wandt, and asked the professor if he could think of another case that resembled the order in the current Apple case.

Wandt mentioned two: The Wireless Communications and Public Safety Act of 1999, which was designed to force cell providers to be able to locate all of their cell phones at all times, and the case of Riley v. California. The latter example was decided in 2014 when the Supreme Court stated that mobile phones present a special challenge to privacy. The Court said, "that your average phone today has so much information in it, and is such a digest and diary of somebody's life, that it needs more protection than it had in the past."

Indeed, our phones carry personal images, fitness and menstrual cycle trackers, saved passwords, work files, and they complicate things further because a company's privacy may be compromised — other people's contact information, personal calendars, access to career apps such as LinkedIn, and many more.

When the FBI or another government organization receives a warrant for a person's home, it's a one-time access to that home. To continue with the analogy, the firmware requested by the FBI would allow investigators to simply walk into a person's digital "house" whenever they thought it was necessary, something that defies the Fourth Amendment in the physical world. Many argue that we're entitled to the same amount of protection against unreasonable searches and seizures in the virtual world. We also have the right to privacy against criminals who might use the same technology to steal from us.

Some have accused Cook and Apple of favoring one person's privacy over the safety of the American public — I'm looking at you, Arkansas Sen. Tom Cotton (R) — but Cook assures the public that this is simply not the case.

"We have no sympathy for terrorists. But now the U.S. government has asked us for something we simply do not have, and something we consider too dangerous to create."

The FBI isn't giving up, but thankfully, Apple's refusal to cooperate has forced investigators to seek alternate routes that don't put the rest of us in danger. We've won this round.

What are your thoughts on the situation?