TIME

This Is the Real Reason Apple Is Fighting the FBI

If the FBI wins, it could open the door to massive surveillance

Julian Sanchez

February 18, 2016

The first thing to understand about Apple's latest fight with the FBI—over a court order to help unlock the deceased San Bernardino shooter's phone—is that it has very little to do with the San Bernardino shooter's phone.

It's not even, really, the latest round of the Crypto Wars—the long running debate about how law enforcement and intelligence agencies can adapt to the growing ubiquity of uncrackable encryption tools.

Rather, it's a fight over the future of high-tech surveillance, the trust infrastructure undergirding the global software ecosystem, and how far technology companies and software developers can be conscripted as unwilling suppliers of hacking tools for governments. It's also the public face of a conflict that will undoubtedly be continued in secret—and is likely already well underway.

First, the specifics of the case. The FBI wants Apple's help unlocking the work iPhone used by Syed Farook, who authorities believe perpetrated last year's mass killing at an office Christmas party before perishing in a shootout with police. They've already obtained plenty of information about Farook's activities from Apple's iCloud servers, where much of his data was backed up, and from other communications providers such as Facebook. It's unclear whether they've been able to recover any data from two other mobile devices Farook physically destroyed before the attack, which seem most likely to have contained relevant information.

But the most recent data from Farook's work-assigned iPhone 5c wasn't backed up, and the device is locked with a simple numeric passcode that's needed to decrypt the phone's drive. Since they don't have to contend with a longer, stronger alphanumeric passphrase, the FBI could easily "brute force" the passcode—churning through all the possible combinations—in a matter of hours, if only the phone weren't configured to wipe its onboard encryption keys after too many wrong guesses, rendering its contents permanently inaccessible.

So the bureau wants Apple to develop a customized version of their iOS operating system that permits an unlimited number of rapid guesses at the passcode—and sign it with the company's secret developer key so that it will be recognized by the device as a legitimate software update.

Considered in isolation, the request seems fairly benign: If it were merely a question of whether to unlock a single device—even one unlikely to contain much essential evidence—there would probably be little enough harm in complying. The reason Apple CEO Tim Cook has pledged to fight a court's order to assist the bureau is that he understands the danger of the underlying legal precedent the FBI is seeking to establish.

Four important pieces of context are necessary to see the trouble with the Apple order.

1. This offers the government a way to make tech companies help with investigations. Law enforcement and intelligence agencies have for years wanted Congress to update the Communications Assistance for Law Enforcement Act of 1992, which spells out the obligations of telephone companies and Internet providers to assist government investigations, to deal with growing prevalence of encryption—perhaps by requiring companies to build the government backdoors into secure devices and messaging apps. In the face of strong opposition from tech companies, security experts and civil liberties groups, Congress has thus far refused to do so.

By falling back on an unprecedentedly broad reading of the 1789 All Writs Act to compel Apple to produce hacking tools, the government is seeking an entry point from the courts it hasn't been able to obtain legislatively. Moreover, saddling companies with an obligation to help break their own security after the fact will raise the cost of resisting efforts to mandate vulnerabilities baked in by design.

2. This public fight could affect secret orders from the government. Several provisions of the federal laws governing digital intelligence surveillance require companies to provide "technical assistance" to spy agencies. Everything we know suggests that government lawyers are likely to argue for an expansive reading of that obligation—and may already have done so. That fight, however, will unfold in secret, through classified arguments before the Foreign Intelligence Surveillance Court. The precedent set in the public fight may help determine how ambitious the government can be in seeking secret orders that would require companies to produce hacking or surveillance tools meant to compromise their devices and applications.

3. The consequences of a precedent permitting this sort of coding conscription are likely to be enormous in scope. This summer, Manhattan District Attorney Cyrus Vance wrote that his office alone had encountered 74 iPhones it had been unable to open over a six-month period. Once it has been established that Apple can be forced to build one skeleton key, the inevitable flood of similar requests—from governments at all levels, foreign and domestic—could effectively force Apple and its peers to develop internal departments dedicated to building spyware for governments, just as many already have full-time compliance teams dedicated to dealing with ordinary search warrants.

This would create an internal conflict of interest: The same company must work to both secure its products and to undermine that security—and the better it does at the first job, the larger the headaches it creates for itself in doing the second. It would also, as Apple's Cook has argued, make it far more difficult to prevent those cracking tools from escaping into the wild or being replicated.

4. Most ominously, the effects of a win for the FBI in this case almost certainly won't be limited to smartphones. Over the past year I worked with a group of experts at Harvard Law School on a report that predicted governments will to respond to the challenges encryption poses by turning to the burgeoning "Internet of Things" to create a global network of surveillance devices. Armed with code blessed by the developer's secret key, governments will be able to deliver spyware in the form of trusted updates to a host of sensor-enabled appliances. Don't just think of the webcam and microphone on your laptop, but voice-control devices like Amazon's Echo, smart televisions, network routers, wearable computing devices and even Hello Barbie.

The global market for both traditional computing devices and the new breed of networked appliances depends critically on an underlying ecosystem of trust—trust that critical security updates pushed out by developers and signed by their cryptographic keys will do what it says on the tin, functioning and interacting with other code in a predictable and uniform way. The developer keys that mark code as trusted are critical to that ecosystem, which will become ever more difficult to sustain if developers can be systematically forced to deploy those keys at the behest of governments. Users and consumers will reasonably be even more distrustful if the scope of governments' ability to demand spyware disguised as authentic updates is determined, not by a clear framework, but a hodgepodge of public and secret court decisions.

These, then, are the high stakes of Apple's resistance to the FBI's order: not whether the federal government can read one dead terrorism suspect's phone, but whether technology companies can be conscripted to undermine global trust in our computing devices. That's a staggeringly high price to pay for any investigation.

Julian Sanchez is a senior fellow at the Cato Institute.