FBI fight with Apple is a big farce to get inside your phone

Joshua Kopstein

February 20, 2016

Earlier this week, the U.S. government dropped a bombshell in its ongoing crusade against strong encryption: Acourt order demanding that Apple help the Federal Bureau of Investigation bypass the security features of an iPhone recovered from Syed Rizwan Farook, who, along with his wife, Tashfeen Malik, killed 14 people last December during a mass-shooting in San Bernardino, California.

National Security Agency whistleblower Edward Snowden called it the "the most important tech case in a decade," and in many ways he's absolutely right. Apple has been on the front lines of the tech privacy fight ever since it improved the security of its devices such that no one, not even the company itself, would be technically capable of accessing their stored data. Now, facing a standstill in Congress, the U.S. government has ordered the company to build a custom version of the iOS operating system that would disable the iPhone's security features, allowing FBI investigators to crack the passcode protecting the device by trying every possible combination — a method known as "brute force."

The order is unprecedented. At stake is whether the U.S. government can legally compel a company to create software that sabotages its own products in the name of fighting crime. In a scathing letter posted on Apple's website, CEO Tim Cook announced the company's intent to fight the order, saying it would set a "dangerous precedent" that would be ineffective against criminals and "would hurt only the well-meaning and law-abiding citizens who rely on companies like Apple to protect their data."

What's more, many details of the case cast doubt on the value or existence of data supposedly contained on the device. It suggests the government's real goal is actually *setting* this dangerous precedent — not unlocking a dead criminal's phone.

Evidence of this strategy can be found in the order itself — including in its legal justification, the All Writs Act, a law that was enacted 277 years ago. The Act broadly allows courts to compel individuals and companies to do pretty much anything, as long as it aids the execution of a court order and isn't unreasonably burdensome. Needless to say, its invocation in a case dealing with advanced technology is bizarre and smacks of desperation to many legal scholars. As the CATO

Institute's privacy law expert Julian Sanchez puts it, "The FBI [...] is relying on an 18th-century law to grant it powers that our 21st Congress won't."

Secondly, the FBI's assertion that the phone contains valuable evidence is at odds with the known facts of the case. The court order notes that Farook destroyed several other phones to hide evidence prior to the attack. It's extremely doubtful he'd neglect to destroy the remaining phone if it had any evidence on it. Another reason to be skeptical: The device was actually owned by Farook's employer, the San Bernardino county health department. Given the lengths he went to destroy evidence, it's highly unlikely Farook would plan attacks using a company device, since it would be reasonable to assume his employer might be monitoring it. The phone was discovered by agents with the "Find My iPhone" feature turned on — a very strange setting to have activated on a device being used to coordinate terrorist plots.

Even more suspicious is how the FBI reacted when finding the phone. According to court documents, they seized the device while it was still on, but allowed the battery to drain. This is baffling because it would have been far easier for investigators to try and access the phone's contents if they had simply kept it powered and turned on. (The device is fully locked with encryption and tamper-prevention measures when turned off)

The government's own descriptions of the information it seeks to obtain by forcing Apple to help unlock the phone are also highly questionable. This crucial information includes "who Farook and Malik may have communicated with to plan and carry out the [San Bernardino] shootings, where Farook and Malik may have traveled to and from before and after the incident, and other pertinent information that would provide more information about their and others' involvement in the deadly shooting."

All of this information could almost certainly be obtained through other, far more constitutionally sound means. "Who Farook and Malik may have communicated with" could be easily determined by issuing a subpoena to their cell phone, email and Internet service providers; those companies all retain customers' calling records and, as we know from the documents Snowden leaked to journalist Glenn Greenwald, regularly provide them to the government. The same point applies to location information, which is constantly gathered by phone companies as customers' cellphones move about and connect to their towers. This too would be obtainable without a warrant. Finally, "other pertinent information … about their and others' involvement" seems like exactly the kind of thing the NSA would be sharing with the FBI during a terrorism investigation. But the story of the shooters has thus far suggested the deranged couple was independently radicalized and had no direct contact with members of the Islamic State abroad.

The case's technical details may be complicated, but Americans should be clear on one thing: The government's goal in this case has little to do with unlocking a single iPhone, and everything to do with establishing a legal precedent that guarantees them the ability to achieve this access on any device.

It's hard to overstate the civil and economic consequences of such a precedent. As Snowden put it, an FBI victory over Apple would result in an "insecurity mandate. A world where Americans

can’t sell secure products, but our competitors can.” And if the U.S. government shows it can compel Apple to help hack its own products, it’s only a matter time before other governments around the world start asking for the same.

Apple is right to stick up for its customers and oppose the U.S. government’s order. The suspicious details surrounding that order only make it a more transparent component of a much broader political agenda — one aiming to eradicate the average person’s ability to protect their data.