

US fight over gunman's locked iPhone could have big impact

February 17 2016, by Eric Tucker And Tami Abdollah



In this photo taken Nov. 15, 2015, Apple CEO Tim Cook speaks in Milan, Italy. A U.S. magistrate judge has ordered Apple to help the FBI break into a work-issued iPhone used by one of the two gunmen in the mass shooting in San Bernardino, California, a significant legal victory for the Justice Department in an ongoing policy battle between digital privacy and national security. Apple CEO Tim Cook immediately objected, setting the stage for a high-stakes legal fight between Silicon Valley and the federal government. (AP Photo/Luca Bruno)

A U.S. magistrate's order for Apple Inc. to help the FBI hack into an iPhone used by the gunman in the mass shooting in San Bernardino, California, sets up an extraordinary legal fight with implications for ordinary consumers and digital privacy.

The clash brings to a head a long-simmering debate between technology companies insistent on protecting digital privacy and [law enforcement agencies](#) concerned about becoming unable to recover evidence or eavesdrop on the communications of terrorists or criminals.

On Wednesday, the White House began disputing the contention by Apple's chief executive officer, Tim Cook, that the Obama administration is seeking to force the software company to build a "backdoor" to bypass digital locks protecting consumer information on Apple's popular iPhones. The early arguments set the stage for what will likely be a protracted policy and public relations fight in the courts, on Capitol Hill, on the Internet and elsewhere.

"They are not asking Apple to redesign its product or to create a new backdoor to one of their products," White House spokesman Josh Earnest said. "They're simply asking for something that would have an impact on this one device."

Within hours of the judge's order on Tuesday telling Apple to aid the FBI with special software in the case, Cook promised a court challenge. He said the software the FBI would need to unlock the gunman's work-issued iPhone 5C would be "too dangerous to create" and called it "undeniably" a backdoor.



This July 27, 2014, photo provided by U.S. Customs and Border Protection shows Tashfeen Malik, left, and Syed Farook, as they passed through O'Hare International Airport in Chicago. A U.S. magistrate has ordered Apple to help the Obama administration hack into an iPhone belonging to one of the shooters in San Bernardino, Calif. The ruling by Sheri Pym on Feb. 16, 2016, requires Apple to supply highly specialized software the FBI can load onto the phone to cripple a security encryption feature that erases data after too many unsuccessful unlocking attempts. Federal prosecutors told the judge they can't access a county-owned work phone used by Farook because they don't know his passcode. (U.S. Customs and Border Protection via AP)

Cook compared it to a master key, capable of opening hundreds of millions of locks, and said there was no way to keep the technique secret once it's developed.

"Once the information is known, or a way to bypass the code is revealed, the encryption can be defeated by anyone with that knowledge," Cook said.

At the center of the debate are the private data carried on nearly 900 million iPhones sold worldwide: Photographs, videos, chat messages, health records and more.

There was swift reaction on the presidential campaign trail, where Donald Trump told Fox News that he agreed "100 percent with the courts," and on Capitol Hill, where the chairman of the Senate Intelligence Committee, Richard Burr, R-N.C., said, "Court orders are not optional and Apple should comply." Democratic Sen. Dianne Feinstein of California, who fought encryption in the 1990s, said she thought the government should be able to access the phone. On Twitter, Edward Snowden called it "the most important tech case in a decade."

But Rep. Justin Amash, R-Mich., called the Justice Department's request "unconscionable and unconstitutional."

The ruling by U.S. Magistrate Judge Sheri Pym represents a significant victory for the Justice Department, which last year decided not to pursue a legislative fix to address encryption but has now scored a win instead in the courts.



An iPhone is seen in Washington, Wednesday, Feb. 17, 2016. A U.S. magistrate judge has ordered Apple to help the FBI break into a work-issued iPhone used by one of the two gunmen in the mass shooting in San Bernardino, California, a significant legal victory for the Justice Department in an ongoing policy battle between digital privacy and national security. Apple CEO Tim Cook immediately objected, setting the stage for a high-stakes legal fight between Silicon Valley and the federal government. (AP Photo/Carolyn Kaster)

Federal officials until now have struggled to identify a high-profile case to make its concerns resonate. But in siding with the government, Pym, a former federal prosecutor, was persuaded that agents investigating the worst terror attack on U.S. soil since Sept. 11 had been hobbled by their inability to unlock the county-owned phone used by Syed Farook, who along with his wife, Tashfeen Malik, killed 14 people in December before dying in a police shootout.

The dispute places Apple, one of the world's most respected companies, on the side of protecting the [digital privacy](#) of an accused Islamic terrorist.

"We have no sympathy for terrorists," Cook said.

Apple has provided default encryption on its iPhones since 2014, allowing any device's contents to be accessed only by the user who knows the phone's passcode. The phone Farook was using, running the newest version of Apple's iPhone operating system, was configured to erase data after 10 consecutive, unsuccessful unlocking attempts.

The magistrate ordered Apple to create special software the FBI could load onto the phone to bypass the self-destruct feature. The FBI wants to be able to try different combinations in rapid sequence until it finds the right one.

The Justice Department said it was asking Apple to help unlock only the iPhone used by Farook and owned by the county government where Farook worked as an environmental inspector. The judge said the software should include a "unique identifier" so that it can't be used to unlock other iPhones. But it was unclear how readily the software could be modified to work against other iPhones, or how quickly Apple might update its own software to render the new bypass ineffective.

"If a court can legally compel Apple to do that, then it likely could legally compel any other software provider to do the same thing," including helping the government install tracking or eavesdropping software on a phone or laptop, said Kevin Bankston, director of the Open Technology Institute at New America.

The next step wasn't immediately clear. The judge gave Apple five days to contest the order as unreasonably burdensome. A magistrate judge on

the lowest rung of the federal judiciary almost certainly could not establish meaningful precedent without affirmation from a higher-court judge, which means the fight is likely to proceed up the chain.

The former head of the FBI division responsible for producing some of the FBI's most cunning surveillance tools, Marcus Thomas, said Apple faces a challenge in showing that the government's request is overly burdensome. Thomas, the chief technology officer at Subsentio LLC, said companies that build ultra-secure products that might be used by criminals or terrorists can expect government requests for help.

"If you're going to build these devices and they're going to be air-tight and you can't get data out of them, then expect to get burdensome requests to help or maybe build solutions," Thomas said. "Society wants to know that companies aren't producing these complicated services and devices that can be used as weapons against them."

© 2016 The Associated Press. All rights reserved.

Citation: US fight over gunman's locked iPhone could have big impact (2016, February 17) retrieved 19 April 2024 from <https://phys.org/news/2016-02-gunman-iphone-big-impact.html>

<p>This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.</p>
--