

Apple and US government head to court over iPhone hack order

March 21 2016, by Brian Melley



This Feb. 17, 2016 file photo shows an iPhone in Washington. The dispute over whether Apple must help the FBI hack into a terror suspect's iPhone is about to play out in a Southern California courtroom. The hearing Tuesday, March 22, in U.S. District Court in Riverside is the first in the battle that has seen Cook and FBI Director James Comey spar over issues of privacy and national security. (AP Photo/Carolyn Kaster,File)

The heavyweight legal fight between the federal government and Apple

Inc. heads to the courtroom after weeks of public sparring over whether the tech giant should be forced to hack into a dead San Bernardino attacker's iPhone.

The sides face off in U.S. District Court in Riverside on Tuesday. They will present witnesses and argue before a magistrate judge who previously ordered Apple to help the FBI crack the code on Syed Rizwan Farook's phone.

The hotly disputed case is in the earliest stage of what is likely to end up at the Supreme Court and set a precedent with broad implications for national security and the reach of law enforcement, as well as the privacy of troves of personal information kept on digital devices.

"What makes this issue hard is that there are security interests on both sides," said Kristen Eichensehr, a visiting law professor at the University of California, Los Angeles. "On the one hand, encryption secures people's communications from prying eyes—criminals, foreign governments and the U.S. government. On the other hand, law enforcement and intelligence agencies seek to serve national security by solving crimes and preventing attacks."

For more than a month, the two sides have waged a very public debate over whether breaking into one phone would jeopardize the security of all encrypted devices.



In this April 30, 2015 file photo, Apple CEO Tim Cook responds to a question during a news conference at IBM Watson headquarters, in New York. The dispute over whether Apple must help the FBI hack into a terror suspect's iPhone is about to play out in a Southern California courtroom. The hearing Tuesday, March 22, in U.S. District Court in Riverside is the first in the battle that has seen Cook and FBI Director James Comey spar over issues of privacy and national security. (AP Photo/Richard Drew, File)

Prosecutors have argued that the phone used by Farook probably contains evidence of the Dec. 2 attack in which the county food inspector and his wife, Tashfeen Malik, slaughtered 14 at a holiday luncheon attended by many of his work colleagues. The two were killed in a police shootout hours later.

The FBI has said the couple was inspired by the Islamic State group. Investigators still are trying to piece together what happened and find out if there were collaborators.

The couple destroyed other phones they left behind and the FBI has been unable to circumvent the passcode needed to unlock the iPhone, which is owned by San Bernardino County and was given to Farook for his job.

Magistrate Judge Sheri Pym last month ordered Apple to create software that would disable security features on the phone, including one that erases all the information if a passcode is incorrectly entered more than 10 times. That would allow the FBI to electronically run possible combinations to open the phone without losing data.

Apple said the government is seeking "dangerous power" that exceeds the authority of the All Writs Act of 1789 it cited and violates the company's constitutional rights, harms the Apple brand and threatens the trust of its customers to protect their privacy. The 18th-century law has been used on other cases to require third parties to help law enforcement in investigations.

The company said the order is unreasonably burdensome. Once created, it would be asked to repeatedly design such software for use by authorities at home and abroad, and the technology could fall into the hands of hackers.

The government has countered that Apple could create the software for one phone, retain it during the process to protect itself, then destroy it. Apple has said that creating software is a form of speech and being forced to do so violates its First Amendment rights.

Both sides have mounted aggressive public relations campaigns to present their side and rhetoric at times has been charged.

Apple CEO Tim Cook ripped the government's "backdoor" approach, a term applied to hackers that has also been used to criticize the way the government eavesdrops on encrypted communications.

FBI Director James Comey rejected talk of seeking a "master key" and said his agency just wants Apple to remove its "vicious guard dog" so it can pick the lock.

"This might be more akin to requiring the person who makes the door to remove the hinges so you can knock the door down," said Riana Pfefferkorn, a cryptography fellow at the Stanford Center for Internet and Society. "Because it would take a long time to kick it in otherwise."

Cindy Cohn, executive director of the Electronic Frontier Foundation, said the government is overreaching.

"It's too much for the government to conscript a company into writing code that undermines the security of the products they sell," she said. "It's not like Apple is saying, 'Go pound sand.' They're saying, 'This is a bridge too far. ... It's dangerous to our security.'"

Law enforcement organizations have weighed in on the side of the Justice Department and called on Apple to help in the investigation. President Barack Obama has said he values privacy but criticized "fetishizing our phones above every other value" and said there had to be some way to get information from the devices.

Other technology heavyweights, such as Google, Facebook, Microsoft and Yahoo, along with civil liberties groups and privacy advocates, have supported one of the world's largest technology companies.

Victims and relatives of the San Bernardino attack have come down on both sides, with some urging Apple to help and others saying privacy concerns are paramount.

While the case gained immense attention, it wasn't the first time the government and Apple have clashed over access to iPhone data.

At the time of Pym's order, a magistrate judge in New York was weighing whether to force Apple to help the government gain access to data on the phone of a methamphetamine dealer. The phone in question, however, used an older operating system than the phone in the San Bernardino case. Apple already has a method to extract data from such phones and had done so at least 70 times for law enforcement.

The San Bernardino case raised the stakes in the fight because Apple says that it's being asked to create a method to access the phone's data that does not exist.

Three weeks ago, the judge sided with Apple, saying prosecutors were stretching an old law "to produce impermissibly absurd results."

The government is now appealing that order and any ruling by Pym is likely to face a challenge that experts expect eventually will go to the Supreme Court.

© 2016 The Associated Press. All rights reserved.

Citation: Apple and US government head to court over iPhone hack order (2016, March 21) retrieved 24 April 2024 from <https://phys.org/news/2016-03-apple-court-iphone-hack.html>

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.