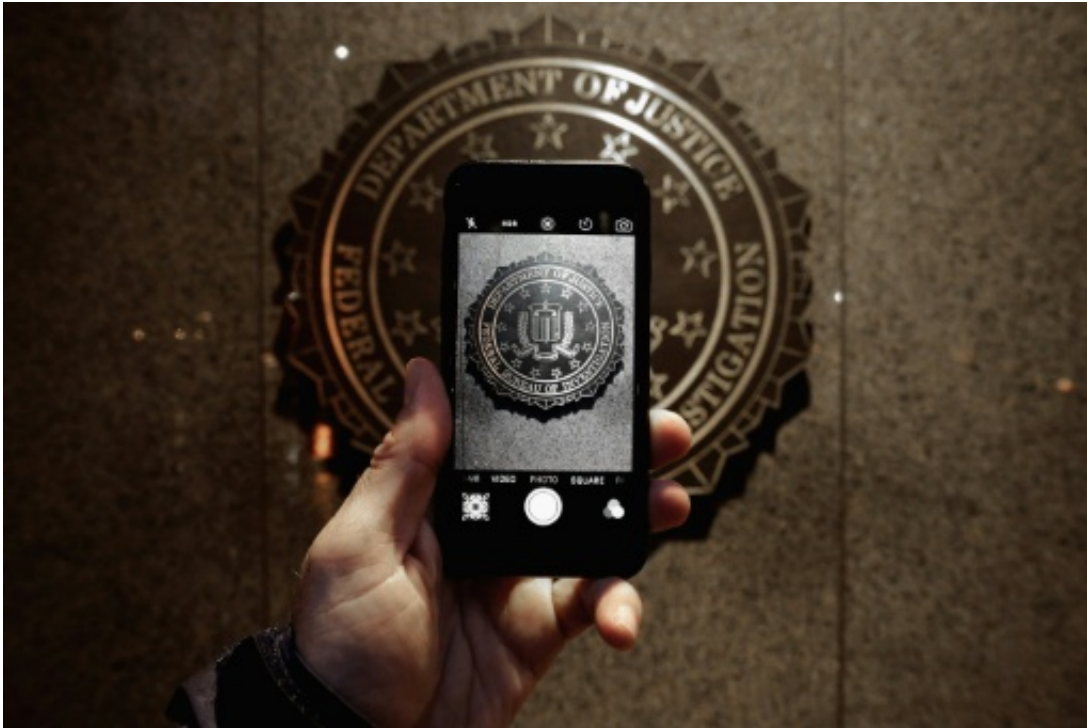


Apple-FBI clash ends in stalemate

March 30 2016, by Rob Lever



Federal prosecutors and Apple for weeks have traded a volley of legal briefs related to the FBI's demand that the tech giant help investigators unlock the iPhone of one of the San Bernardino attackers

The high-stakes legal showdown between Apple and the FBI has abruptly ended, with no resolution to key questions about law enforcement access to devices with strong encryption.

The US government on Monday said it was able to unlock an iPhone used by one of the shooters in the San Bernardino killing rampage, and

withdrew its request for a [court order](#) to force Apple to help break into the device.

The case is over, but not the debate on encryption.

It remains unclear how the FBI and its unnamed "outside party" were able to extract the data being sought, and whether this technique can be repeated on other iPhones with newer versions of the iOS operating system.







"Security is a cat-and-mouse game, and there are bugs fixed in every iOS update, so this development is not surprising to us in the security community," said Joseph Hall, chief technologist at the Center for Democracy & Technology, a Washington advocacy group which has backed Apple in the case.

Hall said that because the US government is pursuing a separate case in New York federal court involving a different iPhone model, that suggests the FBI's hack of the California device may not work in other situations.

"It seems the newer devices might not be vulnerable to this technique," Hall said. "So in the legal sense, this moves from San Bernardino to the (court in the) Eastern District of New York."

FBI vs Apple

How the US government first sought Apple's help, and then hacked an iPhone

2014	December 2, 2015	February 16, 2016	March 21	March 28
<p>Encryption</p> <p>Apple introduces new levels of security on its devices</p>  <p>iOS 8</p> <p>Files are encrypted by default, with the key tied to the user's passcode, which Apple doesn't possess</p> <p>System uses 256-bit AES encryption, considered one of the most secure</p> <p>Data erase</p>  <p>A person trying to guess a password has 10 attempts to get it right, after which the device erases all data stored</p> <p>Source: CNET.com/Mashable/Apple/FBI</p>	<p>Mass murder</p> <p>San Bernardino massacre leaves 14 people dead</p> <p>Suspects Syed Farook (28) and wife Tashfeen Malik (29) are killed in a shootout with police after the attack</p> <p>Farook's iPhone 5C is found by the FBI</p>  <p>FBI asks Apple for help to hack Farook's phone</p> <p>Apple says that it does not have the technical capability to do that</p>	<p>Court orders Apple to help</p> <p>Apple is required to write new code</p>  <p>Apple must build customised iOS software to make it possible to hack Farook's phone without losing data</p> <p>Apple refuses, files an appeal</p>	<p>FBI asks for time</p> <p>On FBI request, appeal hearing postponed</p>  <p>FBI says it may have technical capability to make it unnecessary to force cooperation from Apple</p>	<p>FBI hacks phone</p> <p>FBI no longer needs Apple's assistance</p> <p>FBI says with the assistance of a third party they unlocked the phone</p>  <p>Legal case dropped</p>
		<p>What the FBI wanted</p> <p>Photos, videos, messages, contacts, call history, GPS positions</p> <p>"We simply want the chance, with a search warrant, to try to guess the terrorist's passcode"</p> <p>FBI Director James Comey</p>	<p>What Apple said</p> <p>Once the code exists it would inevitably be hacked</p> <p>"In the wrong hands, this software — which does not exist today — would have the potential to unlock any iPhone"</p> <p>Apple CEO Tim Cook</p>	

AFP

Key issues in the legal and technical showdown between Apple and the US government

Should FBI tell?

Some digital rights activists say the FBI should disclose its method, because it represents a vulnerability that could affect tens of millions of other iPhones in use around the world.

While such a move would appear to go against the FBI's efforts, backers of encryption say disclosure would be in line with a White House policy to inform tech firms of security flaws, to improve overall cybersecurity.

"Since the FBI already got into the phone, if they disclose it to Apple it wouldn't compromise their position if it were just about one phone and not about setting a precedent," said Andrew Crocker of the Electronic Frontier Foundation, which backed Apple's position.

Crocker said the government should release its methods in line with its so-called Vulnerabilities Equities Process revealed in 2014 after a lawsuit by EFF.

"We don't know for sure if this is a vulnerability because the FBI has not talked about it," Crocker told AFP.



Activists gather in front of the US District Court in Riverside, California, on March 22, 2016, where the Apple v FBI trial was due to take place before its sudden postponement

"But if that's the case, the majority of the technical community believes it's generally better to disclose vulnerabilities because we're all at risk if they are not fixed."

Tech companies, security experts and civil liberties advocates had vowed

to fight the government effort, saying forcing Apple to help break into the phone would set a precedent to compel companies to build "backdoors" into their products.

The government had fired back, insisting that Apple was not above the law and that its request for technical assistance was modest.

A number of security professionals argued that Apple is likely to close any security gap if it has not already done so.

Boost for Apple?

Apple can boast that it stood up to the government to protect data privacy, said Chris McClean, a data security analyst at Forrester Research.



Tech companies, security experts and civil liberties advocates say forcing Apple

to help break into the phone of the San Bernardino shooter would set a precedent to compel companies to build "backdoors" into their products

"Unless we hear that this company discovered a fundamental security flaw in iOS, this doesn't tarnish Apple's privacy brand much at all," McClean said.

The government has not revealed the identity of its outside party, but reports have focused on Israeli forensics firm Cellebrite, which has discussed methods for extracting iPhone data.

Computer forensics specialist Jonathan Zdziarski said it remains unclear if the FBI used a "hardware" hack, which would be difficult to duplicate with a newer iPhone, or a "software" method which could potentially work in other devices.

"What is certain, however, is that the only reason this was possible is because (Syed) Farook chose to use a weak form of security on his iOS device—namely, a numeric pin," Zdziarski said on his blog.

Benjamin Wittes, a senior Brookings Institution fellow and co-chair of a Hoover Institution panel on technology and [security](#), said the truce in the encryption war is just temporary.

Wittes, who has supported the government's case, said the legal fight will resume "because sometime soon, there will be a phone the FBI can't break—not even with help from some mysterious outside company."

He added that the debate is also occurring in other countries, such as France, which is considering a law to require law enforcement access to encrypted devices.

The questions of whether companies can built "warrant proof" devices or be compelled to help decrypt them remain unresolved, Wittes said.

"The resolution of this case does not answer any of the questions the case presents," Wittes said on the Lawfare blog.

"Until we answer these questions in the many iterations in which they will present themselves, any relief will be temporary and minor."

© 2016 AFP

Citation: Apple-FBI clash ends in stalemate (2016, March 30) retrieved 29 June 2024 from <https://phys.org/news/2016-03-apple-fbi-clash-stalemate.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.