

FBI: Attacker's phone possibly accessible without Apple help (Update)

March 22 2016, by Brandon Bailey And Amanda Lee Myers



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 government has been adamant for weeks: FBI investigators need to

unlock an encrypted iPhone used by one of the San Bernardino attackers, and Apple Inc. was the only one that could do it.

In a stunning reversal on Monday, federal prosecutors asked a judge to halt a much-anticipated hearing on their efforts to force Apple to unlock the phone. The FBI may have found another way, and Apple's cooperation may no longer be needed, according to court papers filed late Monday, less than 24 hours before Tuesday's hearing.

"An outside party" came forward over the weekend and showed the FBI a possible method to access the data on Syed Rizwan Farook's encrypted phone, according to the filing.

"Testing is required to determine whether it is a viable method that will not compromise data on Farook's iPhone," the filing said. "If the method is viable, it should eliminate the need for the assistance from Apple."

If it's viable, that also means the government has significantly undermined its arguments against Apple, said Kristen Eichensehr, a visiting law professor at the University of California, Los Angeles.

"If they found another way into the phone, that doesn't just weaken their case. It means they can't satisfy the legal standard to sustain the court's order," said Eichensehr, referring to Magistrate Judge Sheri Pym's Feb. 16 ruling compelling Apple to create software that would disable security features on the phone.



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)

Pym granted the government's request to postpone Tuesday's arguments in the case and stayed her previous order. She ordered the government to file a status report by April 5.

The development raised more questions than it answered. It's unclear who is helping the FBI with the phone and why it took so long for a possible solution to be identified.

One thing seems clear—that the government likely would not have

disclosed it had found another possible way to unlock the phone unless it was almost certain the method would work, said Robert Cattanach, a former U.S. Department of Justice attorney who handles cyber-security cases for the Dorsey & Whitney law firm.

He said the disclosure alone weakens the government's case by introducing doubt that it could only access the phone with Apple's help. "They've created ambiguity in a place where they've previously said there is none," he said.

In a conference call with reporters, Apple attorneys said it's premature to declare victory in the case because authorities could come back in a few weeks and insist they still need the company's help. The attorneys spoke under an Apple policy that wouldn't allow them to be quoted by name.

The company hopes the government will tell Apple about whatever method it uses to access the phone's encrypted files. But the attorneys said it may be up to the FBI to decide whether to share the information.

Lawmakers, civil rights advocates and other tech companies have criticized the FBI for not doing more to try to crack the iPhone itself before seeking to force Apple's hand.

"To me, it suggests that either the FBI doesn't understand the technology or they weren't giving us the whole truth when they said there is no other possible way" of examining the phone without Apple's help, said Alex Abdo, staff attorney for the American Civil Liberties Union. "Both of those are scary to me."

The ACLU has filed a court brief supporting Apple's position.

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.

Apple has argued that the government was 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.

It's not clear what method the government now wants to test. But even as the FBI has insisted that only Apple is able to provide the help it needs, some technical experts have argued there are other options.

The most viable method involves making a copy of the iPhone's flash memory drive, said Jonathan Zdziarski, a computer expert who specializes in iPhone forensics. That would allow investigators to make multiple tries at guessing the iPhone's passcode. A security feature in the phone is designed to automatically erase the data if someone makes 10 wrong guesses in a row.

But if that happens, Zdziarski said, investigators could theoretically restore the data from the backup copy they have created.

The data itself would remain encrypted until the phone is unlocked, but it would remain viable while investigators continued to guess the passcode, he added.

"It's a lot more involved than it sounds," Zdziarski cautioned, and no one has demonstrated that it would work in this case.

Some experts have also suggested that investigators could use lasers and acid to deconstruct the phone's memory chip, in order to physically examine the encrypted data and the encryption algorithm, in hopes of cracking the code. But hardware experts say that method has a high risk of destroying the memory during the process.

© 2016 The Associated Press. All rights reserved.

Citation: FBI: Attacker's phone possibly accessible without Apple help (Update) (2016, March 22) retrieved 25 April 2024 from <https://phys.org/news/2016-03-fbi-iphone-apple.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.