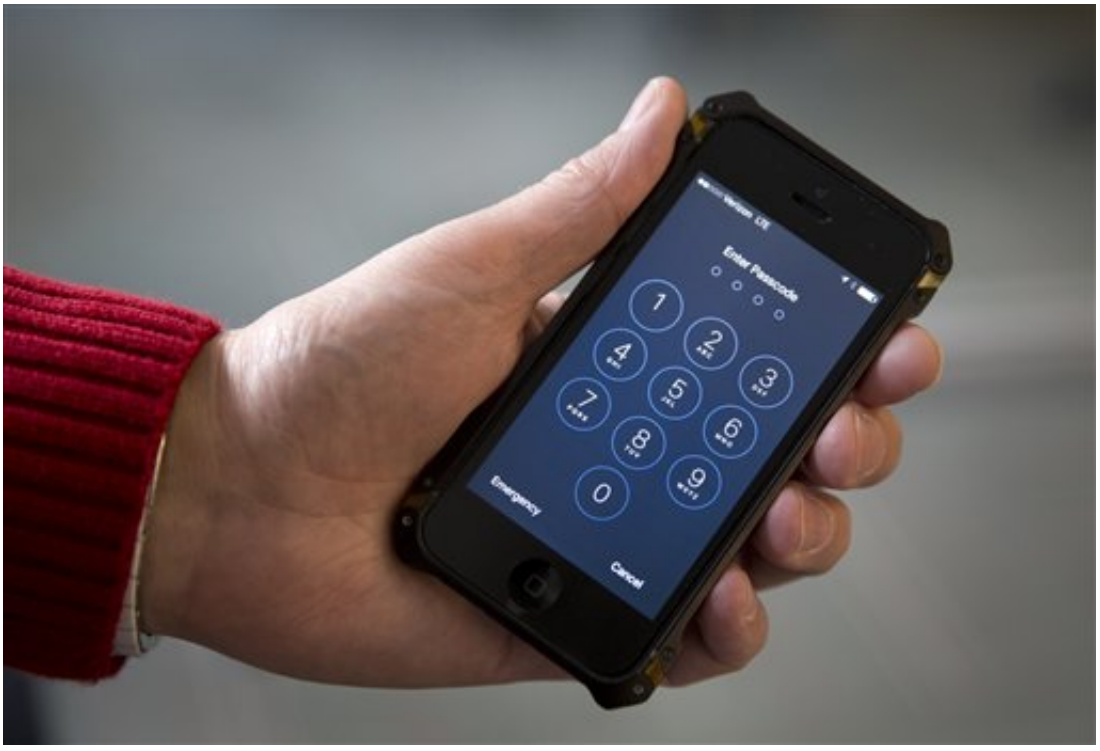
Apple remains in dark how FBI hacked iPhone without its help

March 29 2016, by Tami Abdollah



In this Feb. 17, 2016 file photo, an iPhone is seen in Washington. The FBI's announcement that it mysteriously hacked into an iPhone is a setback for Apple and increases pressure on the technology company to restore the security of its flagship product. (AP Photo/Carolyn Kaster, File)

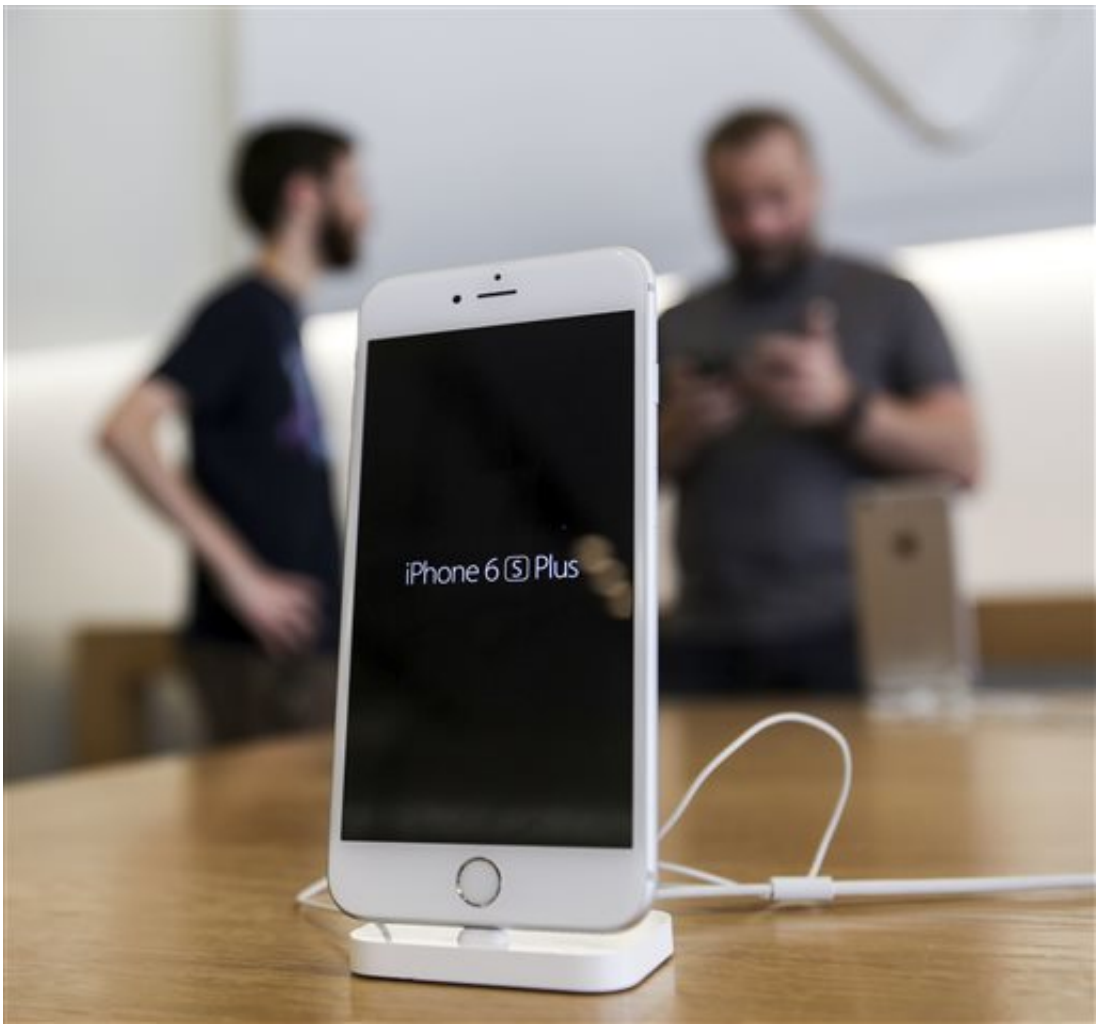
The FBI's announcement that it mysteriously hacked into an iPhone is a public setback for Apple Inc., as consumers suddenly discover they can't keep their most personal information safe. Meanwhile, Apple remains in

the dark about how to restore the security of its flagship product.

The government said it was able to break into an iPhone used by a gunman in a mass shooting in California, but it didn't say how. That puzzled Apple software engineers—and outside experts—about how the FBI broke the digital locks on the phone without Apple's help. It also complicated Apple's job repairing flaws that jeopardize its software.

The Justice Department's announcement that it was dropping a legal fight to compel Apple to help it access the phone also took away any obvious legal avenues Apple might have used to learn how the FBI did it. The Justice Department declined through a spokeswoman to comment Tuesday.

It is a closely held secret how the FBI hacked the iPhone, but a few clues have emerged. A senior law enforcement official told The Associated Press that the FBI managed to defeat an Apple security feature that threatened to delete the phone's contents if the FBI failed to enter the correct passcode combination after 10 tries. That allowed the government to guess the correct passcode by trying random combinations until the software accepted the right one.



In this Friday, Sept. 25, 2015, file photo, an Apple iPhone 6s Plus smartphone is displayed at the Apple store at The Grove in Los Angeles. The FBI said Monday, March 28, 2016, it successfully used a mysterious technique without Apple Inc.'s help to hack into the iPhone used by a gunman in a mass shooting in California, effectively ending a pitched court battle between the Obama administration and one of the world's leading technology companies. (AP Photo/Ringo H.W. Chiu, File)

It wasn't clear how the FBI dealt with a related Apple security feature that deliberately introduces increasing time delays between guesses. The official spoke on condition of anonymity because this person was not

authorized to discuss the technique publicly.

The FBI hacked into the iPhone used by gunman Syed Farook, who died with his wife in a gun battle with police after they killed 14 people in December in San Bernardino, California. The iPhone, issued to Farook by his employer, the county health department, was found in a vehicle the day after the shooting; two personal phones were found destroyed and the FBI couldn't recover information.

The FBI was reviewing information from the iPhone, and it was unclear whether anything useful would be found.

Apple said in a statement Monday that the legal case to force its cooperation "should never have been brought," and it promised to increase the security of its products. CEO Tim Cook has said the Cupertino-based company is constantly trying to improve security for its users.

The FBI's announcement—even without revealing precise details—that it had hacked the iPhone was at odds with the U.S. government's firm recommendations for nearly two decades that security researchers always work cooperatively and confidentially with software manufacturers before revealing that a product might be susceptible to hackers.

Those guidelines lay out a process about how and when to announce that commercial software might be vulnerable. The aim is to ensure that American consumers stay as safe online as possible and prevent premature disclosures that might damage a U.S. company or the economy.

As far back as 2002, the Homeland Security Department ran a working group that included leading industry technology industry executives to

advise the president on how to keep confidential discoveries by independent researchers that a company's software could be hacked until it was already fixed. Even now, the Commerce Department has been trying to fine-tune those rules to protect the digital economy. The next meeting of a conference on the subject is April 8 in Chicago and it's unclear how the FBI's behavior in the current case might influence the government's fragile relationship with technology companies or researchers.

The industry's rules are not legally binding, but the government's top intelligence agency said in 2014 that such vulnerabilities should be reported to companies.

"When federal agencies discover a new vulnerability in commercial and open source software - a so-called 'zero day' vulnerability because the developers of the vulnerable software have had zero days to fix it - it is in the national interest to responsibly disclose the vulnerability rather than to hold it for an investigative or intelligence purpose," the Office of the Director of National Intelligence said in a statement in April 2014.

The statement, which referenced new guidelines by the Obama administration on such disclosures, recommended generally divulging such flaws to manufacturers "unless there is a clear national security or law enforcement need."

Last week a team from Johns Hopkins University said they had found a security bug in Apple's iMessage service that would allow hackers under certain circumstances to decrypt some text messages. The team reported its findings to Apple in November and published an academic paper after Apple fixed it.

"That's the way the research community handles the situation. And that's appropriate," said Susan Landau, professor of cybersecurity policy at

Worcester Polytechnic Institute. She said it was acceptable for the government to find a way to unlock the phone but said the government should reveal its method to Apple.

Mobile phones are frequently used to improve cybersecurity in the private sector or federal agencies, for example, as a place to send a backup code to access a website or authenticate a user for a work system.

The chief technologist at the Center for Democracy and Technology, Joseph Lorenzo Hall, said keeping details secret about a flaw affecting millions of iPhone users "is exactly opposite the disclosure practices of the security research community. The FBI and Apple have a common goal here: to keep people safe and secure. This is the FBI prioritizing an investigation over the interests of hundreds of millions of people worldwide."