theguardian

Government keeping its method to crack San Bernardino iPhone 'classified'

Danny Yadron

March 22, 2016

A new method to crack open locked iPhones is so promising that US government officials have classified it, the Guardian has learned.

The Justice Department made headlines on Monday when it postponed a federal court hearing in California. It had been due to confront Apple over an order that would have forced it to write software that would make it easier for investigators to guess the passcode for an iPhone used by San Bernardino gunman Syed Farook.

The government now says it may have figured out a way to get into the phone without Apple's help. But it wants that discovery to remain secret, in an effort to prevent criminals, security researchers and even Apple itself from reengineering smartphones so that the tactic would no longer work.

Currently, the Justice Department is still testing to make sure the method doesn't damage or erase data stored on devices before using it on Farook's phone. The technique does successfully allow the government to get inside locked iPhones, the Guardian has confirmed.

US officials quickly realized the discovery could be a mixed blessing, people briefed on the developments said. On the one hand, the government may be able to avoid a controversial legal fight with America's most valuable company. On the other, the government now has to be very cautious about when to use the method, which was provided by an "outside party", according to court filings.

Apple has said repeatedly that data stored on locked iPhones shouldn't be able to be accessed without the user's passcode, which Apple doesn't have. Hacking into a locked smartphone requires exploiting a security flaw in its software, and most technology companies fix these flaws once they learn about them.

If the government decides to regularly use its password-bypassing technique in criminal trials, it risks making the method public every time defense attorneys and courts ask questions about how it is accessing information on a locked device.

The law does allow the government to present sensitive sources and methods under seal – out of the view of the public and, more importantly, Apple. But that protection isn't a guarantee. And like any secret, the more people know, the less likely it is to stay secret.

Apple attorneys said on Monday they would push the government to reveal the nature of their tactic if it is used at trial, though it is unclear what legal mechanism they would have to do so.

This means that the government likely hasn't found a usable panacea to getting around iPhone encryption, as there may be many cases where it decides using the tactic isn't worth the risk.

"There are going to be some really interesting and difficult questions between state and local law enforcement agencies," said Christopher Soghoian, principal technologist with the American Civil Liberties Union. "This is a capability the FBIhasn't had for a number of years."

The Justice Department declined to comment.

Assuming the tactic works without erasing phone data, it also means the government is still likely to want the courts or Congress to set firm rules about technology firms' obligations to assist investigations in cases involving encryption. The government will need a more reliable way to access iPhones in more routine cases, and will also face encryption issues in other cases that don't involve iPhones.

Apple privacy battle: defiant Tim Cook vows to defend customers' data

In one non-public case, the US government says it is unable to access messages sent on Facebook's Whatsapp service despite having a court order. That case, previously reported on by the New York Times, is only one of several in which various technology services are a block to federal authorities.

"We'll have to confront these issues again eventually," said Jennifer Granick, director of civil liberties at Stanford Law School's Center for Internet and Society. "It's a temporary victory because it maintains the status quo, which is the FBI can't make Apple do this for now. But it's also just kicking the can down the road."

That may only be more likely after Isis claimed responsibility for Tuesday's attacks in Belgium. Western governments and their allies have increasingly blamed encrypted messaging apps for facilitating Isis communications, though there is no evidence encryption played a role in Belgium.

Julian Sanchez, a privacy law expert at the libertarian-prone Cato Institute, said there may be one benefit for Apple in the government reversing course on the Apple case.

In court filings and in congressional testimony, US officials repeatedly said they knew of no way to get inside Farook's iPhone without the help of Apple. After the government disclosed it found a way into the phone, "it may hurt their credibility for the next time," Sanchez said.