US government delays hearing in Apple iPhone encryption case

Niles Williamson
23 March 2016

The US Justice Department (DOJ) was granted a motion Monday to delay a scheduled federal court hearing in its efforts to compel Apple to unlock an iPhone used by Syed Rizwan Farook, one of the shooters in the San Bernardino attack last December. The government is now claiming that an unnamed third party had potentially developed an alternative means of accessing the encrypted phone

Until the DOJ's filing on Monday, the US government had held that it lacked the means to access the contents of the encrypted phone without the direct assistance of Apple engineers.

The FBI has been seeking to compel Apple to create an alternate operating system which could be installed on the phone and allow it to bypass a lockout feature and carry out a "brute force" hack to gain access to the phone's contents. Once developed, this technology could be used repeatedly by intelligence agencies and police forces to gain access to any iPhone.

The US government is seeking to use Farook's phone as a test case to set a precedent for effectively undermining existing encryption technologies that shield electronic communications from government surveillance.

The government's attorneys did not specify in their court filings what method may have been developed. They argued, however, that the FBI would need additional time to run tests to determine if it was viable and would file a status report on April 5. If the tests show that the method works then, according to court documents, "It should eliminate the need for the assistance from Apple."

NSA whistleblower Edward Snowden, who leaked documents detailing extensive US electronic surveillance operations in 2013, has publicly questioned whether or not the FBI was acting in good faith in its quest to force Apple to open the phone. Responding to the delay in the case on Monday, Snowden tweeted, "Every credible expert knew there were alternative means. That #FBI went so far on so little demonstrated a disregard of facts: bad faith."

There are a number of possible explanations for the government's request to delay the case, including its access to methods to reset the counter that locks out the phone after a limited number of attempts to guess the password, or the discovery of another previously unknown vulnerability in the iPhone iOS operating system by the NSA or other hackers outside the government.

It is also possible that the FBI is bluffing in an effort to allow more time for public concern to die down, or that a secret deal has been reached with Apple to maintain the company's public image of protecting its customers privacy while giving the government access to the phone.

The controversy over encryption erupted last month when Apple CEO Tim Cook, citing privacy concerns, publicly opposed a court order that it develop technology that could be used to create a "backdoor" for the iPhone.

While government officials have publicly insisted that they are not seeking to set a precedent, Cook made clear in an open letter published last month that if Apple was compelled to open Farook's phone it would set a legal and technical precedent for the government to demand that technology companies provide the means to hack any phone on demand.

Even as the US government operates a massive dragnet surveillance operation through the NSA and other agencies, it is seeking complete access to all electronic communications wherever they are transmitted or stored. To this end the Obama

administration has been waging a public campaign against encryption, claiming that technologies that make communications inaccessible to government surveillance are being exploited by terrorists and other criminals.

Speaking at the South by Southwest festival in Austin, Texas last week, President Barack Obama postured as a defender of civil liberties and privacy while backing the efforts to nullify encryption technologies. Obama declared that that technologies that “make possible an impenetrable device or system where the encryption is so strong that there’s no key”—i.e., communications that can not be accessed by the government—play into the hands of child pornographers, terrorists and tax dodgers. “There has to be some concession to the need to be able to get into that information somehow,” Obama said.