FBI claims successful hack of Apple iPhone security systems

By Thomas Gaist
30 March 2016

The Federal Bureau of Investigation (FBI) announced Monday that it successfully hacked security features embedded in the iPhone's iOS 9 operating system, and will therefore end its legal case against the tech giant Apple. In a short court filing, the FBI informed the court that it "no longer requires the assistance of Apple, Inc" in its efforts to compromise the phone's data protection mechanisms.

The government refused to reveal the means by which FBI investigators gained access to San Bernardino gunman Syed Farook's iPhone. While dropping this specific legal challenge, the FBI will continue efforts to employ "the creativity of the public and private sector" toward overcoming any obstacles to its investigation posed by iPhone security software, the government brief stated.

"It remains a priority for the government to ensure that law enforcement can obtain crucial digital information to protect national security and public safety," government attorneys wrote.

The FBI's case, launched with the backing of the Obama administration in February, had sought to force Apple to design and install software that would give investigators access to security systems embedded in an iPhone belonging to San Bernardino shooter Farook.

The agency claimed that its latest efforts to compromise iPhone security were strictly related to the necessities of its investigation of the December 2015 incident.

"The San Bernardino case was not about trying to send a message or set a precedent; it was and is about fully investigating a terrorist attack,'' top FBI official James Comey argued in an op-ed piece published by *Lawfare* last week.

In reality, the case represents the latest manifestation of the Obama administration's drive to seize on the high-profile terror attacks in Paris, San Bernardino, and now Brussels to renew its push for unfettered access to encrypted communications.

Comey practically acknowledged as much in his commentary, arguing in the most general terms for Americans to revise their understanding of "liberty" in accordance with the needs of the security agencies.

"We have awesome new technology that creates a serious tension between two values we all treasure: privacy and safety," he said. "Finding the right place, the right balance, will matter to every American for a very long time."

What exactly Comey means by "the right balance" was already clear from his relentless efforts, waged on behalf of the Obama White House, to promote new legislation requiring companies to install "backdoor" access to their encryption systems.

Beginning with his July 2015 report to the Senate Intelligence Committee, "Counterterrorism, Counterintelligence and the Challenges of Going Dark," Comey staged a series of public appearances in which he issued dire warnings about the horrific terror attacks and crimes that would result from the continued use of unbreakable encryption.

Comey's protestations over the supposed security threat arising from the FBI's lack of access to electronic data are preposterous. In light of everything that has been revealed since the 2013 exposures by Edward Snowden, it is impossible to believe that the FBI's decision to provoke a highly public conflict with Apple over a single iPhone was motivated by purely forensic considerations. The FBI and numerous other federal and state police agencies enjoy sweeping access to vast amounts of electronic data captured by the National Security Agency's mass surveillance programs.

Monday’s decision to suddenly call off the case has only underscored that the suit against Apple was little more than a cynical ploy in service of these efforts to roll back basic democratic rights.

More than simply gaining access to the data on Farook’s phone, which apparently was not far beyond the bureau’s capabilities, the FBI suit has served to ratchet up pressure on Apple and the US tech industry generally.

For its part, Apple resisted the FBI demands only because they were leveled in an intentionally public manner. Apple’s long record of collaboration with US government spying makes clear that the company has no scruples about enabling illegal government surveillance, and the tech companies have been involved in close negotiations with the state for months aimed at working out new forms of cooperation.

“We will continue to help law enforcement with their investigations, as we have done all along,” Apple noted in its statement Monday.