FBI paid more than $1.4m for iPhone hack

21. April 2016

Murad Ahmed, ft.com

The FBI paid more than $1.4m to hackers who developed a way to gain access to the iPhone used by one of the San Bernardino attackers, leading the law enforcement agency to drop litigation against Apple intended to force the company to help break into the device.

James Comey, director of the FBI, said on Thursday that the cost was “worth it”, but added that an accommodation needed to be made with Apple and other technology companies in the future, as paying outside technologists to find ways to access highly-encrypted messages on phones used by terrorist suspects was not “scalable.”

In February, the justice department brought legal action against Apple in an attempt to force the company to create software that would help the FBI break the passcode of the iPhone used by one of the killers in December’s shootings in San Bernardino, California.

Apple resisted the order, saying it would create a “back door” that would harm the privacy of all iPhone users. The FBI dropped the case in March, saying it had found another way to unlock the device but it has not yet disclosed what method it used to do so.

Speaking at an Aspen Security Forum event in London on Thursday, Mr Comey said: “We were able to get into the phone because, in an odd way, all the controversy around the litigation stimulated a marketplace around the world . . . for people trying to figure out if they could they break into Apple 5C running iOS9 - and those details matter because that’s the phone that the terrorists left behind.”

He added that: “Somebody approached from outside the government [with a solution]. We tested it and tested it, then we purchased it.”

Asked how much the FBI paid, he said: “A lot. More than I will make in the remainder of this job, which is seven years and four months, for sure. But it was, in my view, worth it . . . I think it was very, very important that we got into that device.”

Mr Comey’s annual salary was $183,800 last year, suggesting his agency paid about $1.4m to the as-yet-unknown hackers who developed the method to break into the device.

The FBI director added that he wanted to find a long-term solution with technology groups such as Apple and Facebook, which both used end-to-end encryption on some of their messaging services, to avoid the need to pay outside parties if confronted with a similar situation in the future.

“I’m hoping we can get to a sensible solution that doesn’t involve hacking and that doesn’t involving spending loads of money,” he said.

As a former US deputy attorney-general, Mr Comey became a hero among privacy activists when it emerged he resisted the Bush Administration's attempts to gain legal approval for its programme of warrantless electronic surveillance.

But in recent weeks, Mr Comey has lead the US government's charge against the American tech industry and its application of tough security and encryption on smartphones.

US authorities has already signalled the likelihood of future legal clashes with Apple and other tech companies over the use of encryption, which makes it nearly impossible for third parties to intercept messages.

In April, the US Department of Justice said it would attempt to compel Apple to unlock an iPhone seized by police in New York during a drugs investigation. Apple said it was disappointed but not surprised that the government was proceeding with the case, with the company's legal team saying the government was attempting to establish a sweeping precedent that could apply to all phones.

Mr Comey has also said he was "personally" overseeing the investigation into Hillary Clinton's use of a private email servicer while at the State Department, a move that could see him have a big influence over the presidential campaign.

"There's no timetable on any investigation," he said on Thursday. "Somebody asked me in the United States, is the Democratic National Convention [when Mrs Clinton may be elected the Democratic party's nominee for president] a hard stop for you? I say no. We want to do investigations well and do them promptly."