FBI director, Apple lawyer testify before Congress on encryption dispute

Barry Grey
2 March 2016

Federal Bureau of Investigation Director James Comey and Bruce Sewell, vice president and general counsel of Apple Inc., testified Tuesday before the Judiciary Committee of the House of Representatives on the efforts of the Obama administration to eviscerate encryption protection for users of cell phones and other communication devices.

It was the first congressional hearing held specifically on the conflict that has erupted between the Obama administration and the biggest tech company over the government's drive to obtain backdoor access to private encrypted information on cell phones.

On February 16, a federal court in California granted a Justice Department request for an order requiring Apple to write new software enabling the FBI to bypass security features and crack the iPhone of Syed Rizwan Farook, one of the shooters in the San Bernardino attack that killed 14 people last December 2. Apple refused to comply with the order and last week filed an appeal with the court, charging that compliance would set an illegal and unconstitutional precedent for the government to gain access to the personal information stored on the cell phones of millions of people in the US and around the world.

The administration, which decided last fall not to pursue legislation in Congress to compel tech companies to help it gain access to encrypted information, seized on the terror attack in San Bernardino as the occasion for a highly public campaign, utilizing the courts, aimed at overwhelming and intimidating broad popular opposition to a further expansion of government police and surveillance powers.

The government's contention is that it must have access to the dead shooter's phone in order to determine if he and his wife were acting in concert with outside groups such as ISIS. This is absurd on its face, since it is well known that the government already has access to metadata on the phone calls, text messages and other electronic communications of every man, woman and child in America and millions more people around the world through the mass data collection programs that were exposed beginning in June 2013 by National Security Agency whistle-blower Edward Snowden.

The administration is pursuing a two-track strategy to undermine encryption protection for cell phone users. It is seeking to obtain sanction via the courts and simultaneously manipulate public opinion to make it easier for Congress to pass legislation giving the government broad authority to override encryption.

Tuesday's hearing was a step toward obtaining congressional authorization. The response of House Judiciary Committee members to the testimony of Comey, Sewell, New York County District Attorney Cyrus Vance, Jr. and Professor of Cybersecurity Policy Susan Landau indicated that a majority on the committee are prepared to support a law compelling Internet and tech firms to provide the government backdoor access to encrypted information.

In the course of his testimony, Comey backed away from previous claims that the California case was unique and a government victory would not set a precedent for further efforts to crack encrypted iPhones. Committee Chairman Bob Goodlatte, Republican from Virginia, asked Comey, "If the FBI is successful in this case, will it set a precedent in many other cases?" Comey replied, "Yes, potentially."

When the ranking Democrat on the committee, John Conyers of Michigan, asked, "If you succeed in this case, will the FBI return in other cases to ask to unlock phones?" Comey said, "Of course." Conyers, who supports Apple in the dispute, complained that the FBI, by seeking a warrant in the San Bernardino case in open court, had preempted discussions in Congress over legislation and sought to "exploit a national tragedy" to make "an end run around this committee."

Ted Poe, Republican from Texas, asked whether the FBI had other phones in its "lawful possession" that it could not access. Comey's response was, "A lot."

In its appeal brief filed last week in the San Bernardino case, Apple revealed that it is already facing demands from the Justice Department to unlock twelve other phones.

In his prepared remarks to the committee, Comey laid out the framework of the government's propaganda in favor of access to encrypted private information by characterizing the

hearing as an opportunity "to discuss the challenges to public safety and national security that have eroded our ability to obtain electronic information and evidence pursuant to a court order or warrant."

He reiterated the claim, "We are not asking to expand the government's surveillance authority," a transparent lie.

Questioning by committee members showed that divisions over the government's assault on encryption straddled party lines, with some of the most obsequious remarks coming from supposedly liberal Democrats. Luis Gutierrez of Illinois told Comey, "If you have a lawful warrant, you should be able to get private information. We are in the same place."

Cedric Richmond, Democrat from Lousiana, asked Comey, "Are we in danger of creating an underground criminal sanctuary?" to which the FBI director replied, "Yes we are."

Jim Sensenbrenner, Republican from Wisconsin, attacked Apple attorney Sewell for appealing to Congress to resolve the encryption dispute while failing to put forward his own specific proposals for legislation. Sensenbrenner then quipped, "We will be very happy to do that, but I can guarantee you won't like the result."

In his opening statement, Sewell began by stressing his firm's record of collaboration with the government, including giving it private customer information. The revelations of Snowden and others have documented the complicity of all of the major tech, Internet and communications companies in the illegal mass spying operations of the NSA and other state agencies.

"When the FBI came to us in the immediate aftermath of the San Bernardino attacks," Sewell said, "we gave all the information we had related to their investigation. And we went beyond that by making Apple engineers available to advise them on a number of additional investigative options."

Sewell denied that commercial considerations were behind the company's decision to draw the line at openly collaborating in the hacking of its own iPhones, but there is no doubt that untold billions in sales and profits are at stake.

New York County District Attorney Vance, a Democrat, gave a hard-line presentation opposing Apple's encryption policy and demanding that the government be given the authority to override encryption protection.

Landau, the cybersecurity expert, spoke in opposition to the government's demands, citing as her authority the NSA, which has declared "end-to-end" encryption to be essential to US national security.

The hearing was held one day after a federal judge in Brooklyn, New York delivered a setback to the administration's anti-encryption offensive, rejecting its appeal for a warrant ordering Apple to unlock the cell phone of a convicted drug dealer.

In his ruling, Judge James Orenstein singled out for attack the Justice Department's use of the All Writs Act, dating from 1789, as the legal basis for its demand that Apple disable its encryption protection. He concluded that the government's interpretation of the act was so far-reaching "as to cast doubt on [its] constitutionality if adopted." The Justice Department is basing its case in connection with the San Bernardino attacks on its novel and extraordinarily expansive interpretation of the same law.

Attorney General Loretta Lynch on Tuesday weighed in on the encryption dispute, attempting to ratchet up the pressure on Apple to give in to the government's demands. Addressing the RSA Cybersecurity Conference in San Francisco, she said she was "disappointed" by the Brooklyn ruling. Employing a phrase used by Comey to cast encryption in a sinister light, she declared, "The going dark problem is a very real threat to law enforcement's mission to protect public safety and ensure that criminals are caught and held accountable."

Meanwhile, bipartisan bills are being introduced in both the House of Representatives and the Senate to give the government the authority to force tech and communications firms to unlock encrypted data. A bill being drafted by the chairman of the Senate Intelligence Committee, Richard Burr, Republican of North Carolina, and the ranking Democrat on the committee, Dianne Feinstein of California, would penalize companies that don't comply with court orders to help authorities hack into encrypted devices.

A competing bill was introduced Monday to create a bipartisan committee called the National Commission on Security and Technology Challenges to consider encryption and cybersecurity legislation. It was jointly sponsored by Representative Michael McCaul, Republican of Texas, who chairs the House Committee on Homeland Security, and Virginia Democratic Senator Mark Warner. In introducing the bill, McCaul said, "Law enforcement clearly needs the ability to gain lawful access to information that can stop future attacks."