FBI director says agency preparing attack on data encryption after the elections

Kevin Reed
5 September 2016

In a lengthy keynote address on August 30, FBI Director James Comey said the federal government is planning to renew its drive to break data encryption in 2017.

He told a group of cyber security specialists at the Symantec Government Symposium in Washington DC that "what we want to do is collect information this year" to prepare enforcement of backdoor government access to private data and devices.

Comey reiterated his previous claim "that the advent of default ubiquitous strong encryption is making more and more of the room that we are charged to investigate dark." He expanded on the "going dark" metaphor—the inability of state agencies to gain access to protected data and communications—and said, "There was always a corner of the room that was dark … that shadow is spreading to more and more of the room."

Expressing the contempt of the state to basic democratic rights, Comey said the issue "has dipped below public consciousness now" and "next year we can have an adult conversation in this country" about it. In other words, the FBI is counting on the corporate news media and Democratic and Republican presidential candidates to conceal from the public the plans for a stepped up assault on democratic rights following the November elections and the inauguration of a new president.

Comey also went on to give an upside-down elaboration of constitutionally protected privacy rights in America. Arguing that the right to privacy can always be trumped by "good reason" and "security" concerns, he made the extraordinary Orwellian statement, "Even our memories are not absolutely private in the United States." As everyone now knows, the US government does not find it necessary to provide any good reasons to spy on its own citizens; it has been doing it regularly and illegally for many years.

The speech was a more public follow-up to a talk Comey gave in Tampa, Florida on May 25 to the Special Operations Forces Industry Conference sponsored by military contractors such as Lockheed Martin, General Dynamics and Northrup Grumman. Comey reported that during the first six months of 2016, the FBI received about 4,000 devices to investigate. "Five hundred of them could not be opened. That number will only grow," he said.

The use of data encryption has been growing rapidly since the 2013 revelations by Edward Snowden of mass electronic surveillance. The former NSA employee exposed how US government agencies were spying on global Internet activity and electronic communications.

In the last three years, strong data encryption—a method not vulnerable to brute-force decryption attacks—has also become standard on smartphones from companies like Apple and Google without users having to do anything.

Meanwhile, people all over the world have been adopting secure mobile apps with end-to-end encryption that prevents government spying on text and voice communications. For example, the texting application called WhatsApp—with communications decipherable only by the sender and receiver—has more than one billion users today, a five-fold increase since 2013.

These encryption trends are viewed by the state as obstacles that must be broken down in the name of "exceptional access."

In December 2015, the FBI went on the offensive against data encryption following the mass shootings in San Bernardino, California. When the iPhone of attacker Syed Farook was found to be encrypted, the FBI filed and won a federal lawsuit to force Apple to

develop special software that would decrypt it. In the end, the FBI used a private hacking team to break into the iPhone only to later admit that there was nothing of use on the device in the first place.

The entire operation was well-prepared, as the FBI and Justice Department had been developing a campaign against strong encryption for the preceding year. Despite vocal opposition from cryptology experts, the technology industry and the general public, the FBI pressed ahead with demands for backdoor access. The San Bernardino events and government sponsored hysteria surrounding the “war on terror” were seized upon as a pretext to force a denouement on the issue.

No confidence can be placed in the FBI director’s claims that there will be a public debate over government access to private information. There should also be no illusions that the tech industry—whose interests are deeply intertwined with the military-intelligence apparatus—will sustain the democratic right to privacy. Any pronouncements of a settlement or government hearings on encryption should be understood as an indication that some kind of dirty compromise is underfoot.