# FBI Director Comey demands “backdoor” access to encrypted data

**Kevin Reed**
**13 July 2015**

In a stepped up effort to provide government spies with “backdoor” access to privately encrypted information, FBI Director James B. Comey gave testimony on July 8 to the Senate Select Committee on Intelligence and—along with Deputy Attorney General Sally Quillian Yates—to the Senate Judiciary Committee.

In a prepared speech titled “Counterterrorism, Counterintelligence and the Challenges of Going Dark,” Comey argued that US laws should be updated to give the FBI, NSA and CIA special access mechanisms into all forms of data and electronic communication. “Going dark” refers to the inability of the state to monitor the communications of those who use encryption or other modern Internet privacy protection techniques.

In his joint statement with Yates to the Senate Judiciary Committee, Comey said, “Our goal at the Department is to work collaboratively and in good faith with interested stakeholders to explore approaches that protect the integrity of technology and promote strong encryption to protect privacy, while still allowing lawful access to information in order to protect public safety and national security.” In other words, the FBI and Obama administration want to establish a legal and technical framework—with the support of Congress and powerful corporate interests—to further undermine democratic rights by breaking into widely used security methods with special access technologies.

As he has done in the past, Comey stated that “going dark” was a life and death matter. He also specifically said that access to encrypted data was needed to monitor the communications of US citizens. This was the case because “upwards of 200 Americans have travelled or attempted to travel to Syria” and join the ranks of ISIL and “homegrown violent extremists who may aspire to attack the United States from within.”

For her part, Yates said in her testimony that the Obama Administration is looking for a mandate with industry support, but it “may ultimately be necessary” to force companies to comply with government access to encrypted content.

As expected, there were Congressional leaders who agreed with Comey. John McCain had no problem, for example, speaking forcefully in favor of police-state measures, “I’ve heard my colleagues, with all due respect, talking about attacks on privacy and our constitutional rights et cetera, et cetera, but it seems to me that our first obligation is the protection of our citizenry against attack, which you agree is growing.”

None of these assertions should be accepted at face value. For 15 years, the threat of imminent terrorist violence has been used by the US government to bully the public and justify a sustained assault on democratic rights. Meanwhile, the relationship of the same state agencies demanding anti-democratic measures to those who have actually carried out terrorist attacks—from 9/11 to the Boston marathon bombing—has never been seriously investigated.

The Obama administration and the domestic and international spying organizations of the US government are alarmed because commonly used data encryption methods are very effective at keeping them—and others, like hackers,—from accessing live communications streams and data at rest.

The most commonly used data encryption technologies involve the creation of both a public key and a private key. The public key is shared by a user with their email correspondents. The correspondents then use the public key to encode messages intended only for the user who, in turn, decodes the received messages with their private key. Access to the private key requires a password only known to the user.

Due to the development of supercomputers, government agencies have acquired the ability to crack the private key password of “weak” encryption technologies with a so-called “brute force attack.” Such attacks involve a mass of successive password guesses until the correct one is found. With “strong” encryption, more complex passwords and longer encryption keys are used such that the brute force capabilities of current supercomputers are exceeded.

What the FBI and Obama Justice Department are demanding is access to private keys without the permission or knowledge of users.

The real drivers behind the US government’s intensified push for universal data access are two important developments:

1) The popular awareness and response to the revelations by former NSA employee Edward Snowden in June 2013 that the US government had built an infrastructure for storing and analyzing all data communications internationally and was spying on individuals, organizations and governments all over

the world.

2) The decisions of tech companies such as Apple and Google to integrate strong encryption technologies into the operating systems of their smartphones by default, making it impossible for the government to access any information on the devices without the user's passcode.

According to Pew Research, in the two years since Snowden's revelations, 87 percent of Americans are aware of the government's illegal data surveillance activities and 34 percent of those who are aware of the programs have taken measures to hide or shield their information from the government. Additionally, the Pew study—published in March of this year—found that 22 percent of all US adults say they have "changed the patterns of their own use of various technological platforms 'a great deal' or 'somewhat' since the Snowden revelations."

The Pew study flies in the face of Comey's testimony when he attacked the public's concern for privacy rights. "I don't exactly know where the great demand for this is coming from," he said. "I haven't met ordinary folks who say, 'I really want a device that can't be opened even if an American judge finds it ought to be opened.'"

Also, data maintained by PGP (Pretty Good Privacy)—the most commonly used data-encryption software for securing private email—shows a steady growth in encryption implementation. The number of people using PGP took a sharp turn upward following the Snowden revelations and has sustained double the rate of daily adoption since then.

Other encrypted communications platforms, such as the popular mobile texting tool WhatsApp, is being used by increasing numbers of people worldwide over the past few years. Reaching more than 800 million users as of April 2015, WhatsApp has been adopted by three-quarters of all mobile users in South Africa, Malaysia, Argentina and Singapore and more than half of mobile users in 12 countries in Europe, the Middle East, Asia and South America.

There has been a vocal opposition by many in the high tech industry to the demands for government access to encrypted data. In the days leading up to and following Comey's testimony at the Capital, industry representatives and advocates for information privacy defended the present data security approach and objected to proposals for any kind of "backdoor." Many of these experts focused on the negative impact on American tech companies in the world market should the US force through any measures to undermine established security practices. Other technology specialists have criticized the Obama administration for having a flawed conception of the data security technology and for putting forward ideas which cannot be effectively implemented.

The Electronic Frontier Foundation, a leading organization that defends civil liberties in the digital world, focused a portion of its analysis on the constitutional implications of the Obama administration's plans. The EFF wrote, "In both hearings the witnesses representing law enforcement trotted out scary hypothetical situations and terrifying anecdotes about how encryption could stifle investigations and let 'bad guys' go free. But when asked by Senators if they had any actual numbers on how often strong encryption thwarted investigations, neither Director Comey nor DAG Yates had any idea."

To the extent that business concerns or "bad science" are advanced as the primary objections to the anti-democratic operations of the US government, the front door is being flung wide open for a compromise on fundamental political rights. Some technologists have already suggested that the government should go back to the drawing board with its "exceptional access" effort and design technical requirements that can be reviewed by academic and industry communities for "weaknesses and hidden costs."

It should be pointed out that the encryption measures taken by Apple and Google, among others, were largely for self-preservation purposes. After the Snowden leaks, major American tech companies spent billions of dollars building overseas data centers in order to combat the impression that the US government would have access to foreign customer data. Meanwhile, the encryption protections that have been implemented on the Apple and Google mobile devices do not apply to the cloud storage services that they offer which remain open to government surveillance.

Recently, some tech industry representatives have circulated the idea of a "golden key" or "split-key" that would store a special key with the government or some third party organization that could be used to decode data and communications at the request of law enforcement. This proposal also includes a court review process much the same as that which has been in place under the Foreign Intelligence Surveillance Act. Another proposal would require tech companies to hand over email metadata—details about communications such as who is being contacted and when the messages are being sent—without looking at the content of the messages.

The differences between the current initiative and what is already in place is that it would officially sanction spying by the US government on its own citizens. Finally, it should not be assumed that because the FBI has renewed its campaign for a sanctioned solution to the "going dark" problem, that something is not already being put in place behind the backs of the American people.