

FBI director demands unfettered access to all encrypted phone data

Thomas Gaist
18 October 2014

In a speech Thursday at the Brookings Institution in Washington DC, titled “Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?” Federal Bureau of Investigation Director James Comey demanded that the major telecommunications corporations develop new “backdoor” access points in their encryption systems to facilitate the US government’s mass surveillance programs.

Comey’s speech exposed the real perspective of the US ruling elite—usually concealed behind the smokescreen of lies—with respect to the unconstitutional surveillance programs run by the National Security Agency, the FBI and other government agencies.

Comey made clear the government will not tolerate even minor and ineffective obstacles to the government’s wiretapping and data mining efforts, such as the limited forms of cell phone encryption promoted by the tech companies as part of a marketing strategy.

Focusing in particular on the deployment of cell phone encryption software by Apple and Google, Comey complained that even with its existing “supercomputer” technology, the government is hampered in its surveillance efforts by increasing use of widely available data encryption methods.

“The law hasn’t kept pace with technology... Encryption threatens to lead all of us to a very dark place,” Comey warned.

Comey acknowledged that the promotion of cellphone encryption by the corporations is motivated by public relations considerations stemming from exposures of NSA spying. Alluding to the attempts of the companies to refurbish their reputations, damaged by revelations from Edward Snowden that they actively collaborated in the government’s mass spying, Comey said, “Encryption isn’t just a technical feature; it’s a

marketing pitch... And my question is, at what cost?”

Comey noted that the companies are defending their new encryption systems by pointing to other methods through which the government can gain access to their customers’ data en masse. “Apple argues, for example, that its users can back-up and store much of their data in ‘the cloud’ and that the FBI can still access that data,” Comey said.

The FBI director insisted, however, that the agency requires direct access to communications content, effectively admitting the fraudulence of US government claims that only metadata is subject to dragnet surveillance.

“Metadata doesn’t provide the content of any communication. It’s incomplete information,” Comey said.

Comey’s comments included a notable departure from the usual platitudes advanced by surveillance boosters about the supposed need to “strike a balance” between “liberty” and “security.” Echoing arguments advanced by the most authoritarian regimes in modern history, the FBI director said that even minimal freedoms can only be protected by a powerful, omnipresent security apparatus.

“Some have suggested there is a conflict between liberty and security. I disagree.... When a city posts police officers at a dangerous playground, security has promoted liberty—the freedom to let a child play without fear,” Comey said.

There is a growing recognition within the US elite that the population is not convinced by surveillance justifications based on the threat of “terrorism.” Comey largely framed his arguments in terms of the need to surveil kidnappers and child abusers, warning of “predators who exploit the most vulnerable among us” and “violent criminals who target our communities,”

while citing a number of particularly horrific incidents in an effort to justify systematic violation of privacy and democratic rights by the state.

Comey's remarks were peppered with blatant lies and distortions about the extent of government surveillance. Brushing aside the avalanche of evidence publicized by Snowden, Comey claimed, absurdly, that the US government is not systematically gathering data on the population.

"In the wake of the Snowden disclosures, the prevailing view is that the government is sweeping up all of our communications. That is not true," Comey said. "Perhaps it's time to suggest that the post-Snowden pendulum has swung too far in one direction—in a direction of fear and mistrust."

Turning reality on its head, Comey claimed that while the government has the necessary "legal authority to intercept and access communications and information," the agency nonetheless lacks "the technical ability to do so."

In fact, as documents leaked by Edward Snowden have conclusively demonstrated, surveillance programs developed by the US government are systematically acquiring, storing and analyzing every bit of communications data produced by populations worldwide. Comey's assertions about "legal authority" notwithstanding, these programs operate in flagrant violation of the US Constitution, the Bill of Rights and international human rights covenants. Near the conclusion of his remarks, Comey pointed to these essential political issues at stake in the struggles over electronic surveillance—those relating to democratic rights and the rule of law—before asserting, in contradiction to all the evidence, that the system of checks and balances established by the framers of the US Constitution remains in force.

"This country was founded by people who were worried about government power... they divided government power among three branches, with checks and balances for each. And they wrote a Bill of Rights to ensure that the 'papers and effects' of the people are secure from unreasonable searches," Comey said.

"The means by which we conduct surveillance through telecommunication carriers... is an example of government operating in the way the founders intended—that is, the executive, the legislative, and the judicial branches proposing, enacting, executing, and

overseeing legislation, pursuant to the rule of law," Comey said.

"I think it's time to ask: Where are we, as a society? Are we no longer a country governed by the rule of law, where no one is above or beyond that law?" Comey asked.

In reality, one of the main "legal" underpinnings for the government's mass spying programs is Executive Order 12333, a unilateral decree promulgated by the Reagan administration and extended by further executive fiats issued during the George W. Bush administration. For its part, the judiciary has been effectively incorporated into the illegal activities of the government through the establishment of the Foreign Intelligence Surveillance Court in 1978, a parallel authoritarian shadow court that routinely rubber-stamps mass surveillance requests submitted by the NSA.

Freed from any meaningful oversight or constitutional constraints, it is the security agencies of the executive branch that increasingly operate as a law unto themselves. As Comey's own remarks Thursday made clear, these instruments of capitalist class rule are determined to access *all of everyone's* data, *all* of the time, viewing with unconcealed hostility any attempt to protect one's "papers and effects" from government scrutiny.



To contact the WSWS and the Socialist Equality Party visit:

wsws.org/contact