Trump administration escalates attack on data encryption

Will Morrow
17 January 2018

The Trump White House is escalating the efforts of the previous Obama administration to circumvent and criminalize encryption of electronic communications and mobile devices used by billions of people around the world.

This was the theme of a speech by Federal Bureau of Investigation (FBI) director Christopher Wray on January 9 in New York City before an audience of technology corporation heads and government officials. Wray referred to the use of electronic encryption as the "going dark problem," a phrase coined by former FBI director James Comey as part of the Obama administration's drive to remove any impediment on government spying. He explained that the issue "comes up in almost every conversation I have with leading law enforcement organizations, and with my foreign counterparts from most countries—and typically in the first 30 minutes."

Wray claimed that the agency had not been able to act upon warrants to search 7,775 electronic devices because it could not break through their encryption. On this basis, he demanded that technology companies install backdoor systems into all of their devices that could be used by the intelligence agencies.

In a speech last October, Deputy Attorney General Rod Rosenstein went even further, singling out not only encryption of electronic devices, but the use of so-called end-to-end encryption in messaging systems, which are incorporated in mobile phone applications such as Whatsapp and Signal by default. The number of people using these applications has exploded to more than one billion, particularly in the wake of Edward Snowden's 2013 exposure of mass NSA spying.

End-to-end encryption relies on the principle of a public-private key system. Each user has a public key which others can use to encrypt messages to them, but which can only be decrypted with the private key that only the user possesses. In principle, this means that even the administrators of the messaging application server cannot access the message contents, because they are encrypted from end to end.

Rosenstein declared that "Billions of instant messages are sent and received each day using mainstream apps employing default end-to-end encryption. The app creators do something that the law does not allow telephone carriers to do: they exempt themselves from complying with court orders."

Rosenstein openly admitted that the government's main concern is not a relatively small number of criminal suspects, but the mass communications of the entire working class. "Encrypted communications and devices pose the greatest threat to public safety," he declared, "when they are part of mass-market consumer devices and services that enable warrant-proof encryption by default."

The deputy attorney general hinted that the Trump administration was moving to criminalize encryption. He complained that the "approach taken in the recent past—negotiating with technology companies and hoping they will eventually assist law enforcement out of a sense of civic duty—is unlikely to work. Technology companies operate in a highly competitive environment. Even companies that really want to help must consider the consequences. Competitors will always try to attract customers by promising stronger encryption."

In other words, the problem facing both the government and the CEOs of technology companies—which are already integrated into the mass surveillance of the population—is that ordinary people are opposed to government surveillance. Rosenstein concluded: "There is no constitutional right to sell

warrant-proof encryption. If our society chooses to let businesses sell technologies that shield evidence even from court orders, it should be a fully-informed decision."

This is the pseudo-legal rationale for dictatorship. The logical corollary of Rosenstein's claim that files and communications are illegal which are "warrant-proof" is that the government must have access to every email, text message, phone call and document of every person in the country. The Fourth Amendment right of the people to be "secure in their persons, houses, papers, and effects, against unreasonable searches and seizures," is rendered meaningless.

Rosenstein's claim that the government is concerned only with communications for which it possesses a warrant is transparently absurd, given that the government already illegally spies on the communications of millions of people, including US citizens, operating with the strategy to "sniff it all, collect it all, know it all, process it all and exploit it all," as one NSA document leaked by Edward Snowden put it. This month, Democrats and Republicans voted together to maintain Section 702 of the Foreign Intelligence Surveillance Act (FISA), which allows for the warrantless spying on individuals outside the US, as well as all of their contacts, including US citizens.

The bipartisan drive to illegalize encryption was escalated under the Obama administration in 2015 in the wake of the November Paris terror attacks and the December mass shooting in San Bernardino, California. The FBI claimed at the time that it could not break the iPhone passphrase of one of the San Bernardino shooters, Syed Rizwan Farook, who was killed by police in the attack.

The Obama administration organized a public lawsuit against Apple in February 2016, to force it to install a new version of the iOS operating system on Farook's phone, which would allow the FBI to crack the phone's passphrase. Apple refused, at least publicly, to do so, arguing that such an action could be replicated on other users' devices and would set a precedent for the government to access the phone of any individual (see: "White House steps up drive to outlaw encryption"). In the end, the FBI dropped the lawsuit because it claimed it had been able to use an unnamed "third party" to crack the phone.

The purpose of the lawsuit was to utilize the initial shock and confusion among the population that accompanies such disasters to mobilize support for an attack on the rights of the entire population. Last November, the Trump administration served Apple with another subpoena to force it to unlock the iPhone of 26-year-old Devin Patrick Kelley, the attacker at the Sutherland Springs, Texas shooting.

The Trump administration's push to criminalize encryption is part of an international campaign. On July 31, UK Home Secretary Amber Rudd called on WhatsApp's owner Facebook to remove end-to-end encryption, arguing that it "aids terrorists." The Australian government has introduced legislation seeking to force companies to provide the contents of encrypted communications.

The ruling class is being driven by its extreme fear of mass opposition to its right-wing policies and a growing political radicalization among workers and young people after more than 25 years of permanent war, growing social inequality, and more than 16 years of attacks on democratic rights under the fraudulent banner of the "war on terror."

In the fight against this campaign, no confidence can be placed in the social media and technology corporations, such as Facebook and Google. While collaborating in mass spying, they are acting in lockstep with governments internationally to suppress growing political opposition by censoring left wing and oppositional websites.