Republicans introduce Senate bill to abolish strong encryption on consumer devices

Kevin Reed
29 June 2020

Three Republican Senators introduced a bill on June 23 that would force tech companies to allow US law enforcement back door access to encrypted data and communications on consumer electronic devices and applications.

Senate Judiciary Committee Chairman Lindsey Graham (Republican from South Carolina), US Senators Tom Cotton (Republican from Arkansas) and Marsha Blackburn (Republican from Tennessee) proposed the draft bill called the Lawful Access to Encrypted Data Act. The senators called the measure a "balanced solution to bolster national security" that would end what they call the "warrant proof" encryption on smartphones, tablets and computers that is used by "terrorists and other bad actors to conceal illicit behavior."

The press release accompanying the introduction of the bill says that it would "require service providers and device manufacturers to provide assistance to law enforcement when access to encrypted devices or data is necessary—*but only after* a court issues a warrant, based on probable cause that a crime has occurred, authorizing law enforcement to search and seize the data."

As has been repeatedly argued by the tech industry and data security experts, there is no way to develop "lawful" access to encryption without breaking the entire system that is now being used—especially in the wake of revelations of illegal government surveillance of electronic communications—by billions of people around the world.

Stopping short of naming specific companies—such as Apple, which has so far refused to grant the FBI or local police departments access to encrypted data on its iPhones—Cotton said of the bill, "Tech companies' increasing reliance on encryption has turned their platforms into a new, lawless playground of criminal activity. Criminals from child predators to terrorists are taking full advantage. This bill will ensure law enforcement can access encrypted material with a warrant based on probable cause and help put an end to the Wild West of crime on the internet."

Senator Cotton's aggressive support for law enforcement access to the everyone's encrypted information comes as no surprise. His advocacy for what will undoubtedly become a "wild west" of state attacks on Fourth Amendment rights against unreasonable searches and seizures is of a piece with his recent call to "send in the troops" to "restore order to our streets" during the protests against police violence across the country.

The draft bill has three components. The first is that it provides the US Department of Justice (DoJ) the authority to require the largest hardware manufacturers, computer and mobile device operating system developers and communications providers to comply with directives to decrypt data upon request. The new law applies to tech companies that sold at least 1 million systems to consumers or had at least 1 million monthly active users in 2016 or any year thereafter.

Second, these qualifying companies must figure out for themselves how to solve the technical problems in complying with a DoJ directive. While the companies can subcontract the solution for law enforcement access to encrypted data to a third party, the firms are required to "bear the costs associated with the development of the capability required."

Last, in a back-handed acknowledgement that the entire conception of law enforcement-only access to encryption is fundamentally flawed, the law absurdly offers a "Prize Competition"—a cash payment of an unspecified amount—for a winning individual, group,

organization or university based in the US that finds "solutions providing law enforcement access to encrypted data pursuant to legal process."

Responding to the introduction of the bill, Attorney General William Barr said, "I am confident that our world-class technology companies can engineer secure products that protect user information and allow for lawful access." In fact, Barr's influence on the bill is obvious as there is a section of it that repeats more or less verbatim the novel legal arguments made by the attorney general last summer against the Fourth Amendment.

The Silicon Valley tech corporations issued a combined statement on Thursday through an organization called Reform Government Surveillance (RGS), which stated, "The Reform Government Surveillance coalition strongly opposes the Lawful Access to Encrypted Data Act. This bill would require companies to build encryption backdoors that would jeopardize the sensitive data of our billions of users and the security of our products and services. It would leave all Americans, businesses, and government agencies dangerously exposed to cyber threats from criminals and foreign adversaries and make us all less safe.

"The global pandemic has forced everyone to rely on the internet in critical ways, making digital security more important than ever before for our economy and national security. Strong encryption provides users, businesses, and our government with the important tools they need to keep us protected."

Members of RGS include Apple, Facebook, Google, Twitter, LinkedIn, Microsoft, DropBox and Snap, Inc and was founded in 2013 in response to the exposure by former intelligence analyst and NSA contractor Edward Snowden of mass US government surveillance of the public.

In a tweet the evening that the bill was introduced, Will Cathcart, head of the Facebook-owned WhatsApp, wrote, "At a time when cyberthreats from criminals, hackers, and nation states are on the rise, our nation's leaders should not be calling on companies to weaken the encryption that allows us to communicate privately and securely." WhatsApp is an end-to-end encrypted communications platform and has 1.5 billion monthly active users—the majority of whom live outside the US—making it the most popular mobile messenger app in the world.

The Electronic Frontier Foundation (EFF) said of the proposed Republican bill, "The bill is sweeping in scope. It gives the government the ability to demand these backdoors in connection with a wide range of surveillance orders in criminal and national security cases, including Section 215 of the Patriot Act, a surveillance law so controversial that Congress can't agree whether it should be reauthorized."

The conflict between the tech companies and the Trump administration—as well as the Obama administration before it—goes back to 2015-2016 when Apple refused to assist the FBI in breaking the encryption on one of the iPhones of the San Bernardino shooters. As has been the case with each of the increasing claims that federal authorities must have unfettered access to encrypted data on-demand to "fight child sex traffickers and terrorists," in the end, the FBI was able to hack the San Bernardino shooter's phone.

The struggle to stop the US government assault on Fourth Amendment rights against unreasonable searches and seizures as it pertains to encrypted private information and communications cannot be left in the hands of the tech monopolies. Motivated by global market share and competitive considerations against rival manufacturers, software developers and communications platforms from other countries, especially China, the corporate decision-makers in Silicon Valley will ultimately drop their rejection of back door access when it comes down to state ultimatums regarding the protection of American "national security interests."

Only the mobilization of the international working class on the basis of the struggle against capitalism and for socialism can defend and protect the democratic rights of the people against intrusions by both the state and the tech giants.