Republican Senator Lindsey Graham introduces bill that threatens end-to-end encryption

Kevin Reed
8 February 2020

Republican Senator Lindsey Graham is circulating a discussion draft bill that would use the enforcement of laws against distribution of child sex abuse material (CSAM) as a means of shutting down end-to-end encryption services provided by the big tech companies.

The bill, which is also reportedly being worked on by Senator Richard Blumenthal (Democrat of Connecticut), would create a 15-member bipartisan National Commission on Child Exploitation Prevention that would be responsible for establishing the rules and overseeing the removal of CSAM content from the internet. The law would make the Attorney General the chairman of the commission and give him or her the authority to modify any of its recommendations.

Called the Eliminating Abusive and Rampant Neglect of Interactive Technologies (EARN IT) Act of 2019, the bill would make technology companies liable for state prosecution and civil lawsuits for child abuse and exploitation content unless they follow "best practices" outlined by the commission.

On January 30, Bloomberg published a draft of the bill noting, "The draft bill from Graham, the South Carolina Republican who chairs the Senate Judiciary Committee, mounts a double attack against encrypted services such as Apple Inc.'s iCloud and Facebook Inc.'s WhatsApp chat. It jeopardizes technology companies' immunity to lawsuits by victims for violating child exploitation and abuse statutes and it lowers the standard to bring such cases."

At the heart of the proposed law is an attack on what is known as Section 230 of the Communications Decency Act which protects providers of computing devices, apps and internet services from liability for content copied or posted by users onto their products. Companies that refuse to follow the commission's best practices will lose their Section 230 protections for any content deemed to violate the content rules set by the commission.

Although the draft bill does not specify any of the rules, it is transparently obvious that it would require law enforcement immediate and unfettered access to devices, communications and cloud accounts. As has been explained by technology experts, the bill's references to law enforcement "identifying, categorizing, and reporting material related to child exploitation or child sexual abuse" would be impossible to do on devices and services with end-to-end encryption.

End-to-end encryption is the popular method used by the consumer technology corporations of protecting electronic communications and data stored on computer devices by using cryptographic keys to block eavesdropping, surveillance and interception of information. The use of end-to-end encryption by the public, corporations and other organizations has been on the rise since the exposures by Edward Snowden in 2013 that the US government was capturing and storing the mobile phone and email communications of the entire population in a massive and illegal electronic dragnet.

Companies such as Apple and Facebook have been deploying end-to-end encryption in their products by default for several years now. Apple has battled publicly with the Justice Department several times since 2014 over demands by the FBI for back-door access to the encrypted iPhones of mass shooters.

In the most recent of these incidents, the shooting at

the naval base in Pensacola, Florida, on December 6, it emerged that Apple had actually begun to cave into the demands from Attorney General William Barr and President Donald Trump for law enforcement access and a backdoor to encrypted data and communications.

As reported by Reuters at the time, “Apple did in fact turn over the shooter’s iCloud backups in the Pensacola case, and said it rejected the characterization that it ‘has not provided substantive assistance.’ Behind the scenes, Apple has provided the U.S. Federal Bureau of Investigation with more sweeping help, not related to any specific probe” by dropping plans to offer consumers the ability to fully encrypt their iCloud backups.

Clearly, Senator Graham, the US Justice Department and others are attempting to exploit public fears and concerns about child sexual abuse as a means of pushing through their agenda for the abolition of encryption that has been underway for five years. As Riana Pfefferkorn of the Center for Internet and Society at Stanford Law School explained, “This bill is trying to convert your anger at Big Tech into law enforcement’s long-desired dream of banning strong encryption. It is a bait-and-switch. Don’t fall for it.”

Gizmodo, the technology and science site, wrote on January 31, “It doesn’t take a genius to see where this is going. The federal government, and especially the DOJ, have wanted tech companies to build surveillance backdoors into their end-to-end encrypted messaging services for years. They insist that they are only interested in preventing major crimes like terrorism or sex trafficking, but in reality, building those backdoors would create a convenient pipeline for domestic surveillance.”

The technique of exploiting the public disorientation caused by terrorist violence and other criminality by the state to attack fundamental democratic rights has been employed increasingly by the political, law enforcement and national intelligence establishment since the events of September 9, 2001.

The provisions of Section 230 of the Communications Decency Act were adopted in 1996 (also known as Title V of the Telecommunications Act of 1996) which state, “No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.” This section of the 1996 legislation was, in part, a response to the growth of the internet and has been frequently referred to as a key to the flourishing of the World Wide Web and sometimes as “The Twenty-Six Words That Created the Internet.”

The intensifying assault on end-to-end encryption is part of the ongoing drive by the state to censor and regulate content on the internet. Democrats, in particular, have led the campaign against big tech with Senator Elizabeth Warren, Democrat of Massachusetts and candidate for the party’s 2020 presidential nomination, campaigning since March 2019 for a “break up” of the tech monopolies.

There has also been a steady campaign conducted by the *New York Times*, under the guise of the fight against so-called “surveillance capitalism,” to utilize the egregious privacy violations carried out by the tech monopolies to mobilize the public behind government censorship of online content. Significantly, none of these initiatives warn the public about the role of the state and military-intelligence apparatus in utilizing artificial intelligence and the communications infrastructure to spy on the entire population.