

Senate Judiciary Committee unanimously approves anti-encryption EARN IT Act

Kevin Reed
16 July 2020

The Senate Judiciary Committee voted on July 2 to send an amended draft of the EARN IT Act—a bill that both attacks free speech and surreptitiously abolishes encrypted electronic communications—to the Senate floor prior to leaving for the two-week Fourth of July recess.

The Eliminating Abusive and Rampant Neglect of Interactive Technologies Act of 2020 (EARN IT), which falsely claims to protect children from online sexual abuse, was approved unanimously by twelve Republicans and ten Democrats on the committee.

The modified bipartisan legislation was co-sponsored by Committee Chair Lindsey Graham (Republican of South Carolina) and US Senator Richard Blumenthal (Democrat of Connecticut) and approved after two amendments had been introduced to it.

The first of these changes removed the Department of Justice as the government body charged with enforcing the “best practices” proposed by a national commission for websites, social media platforms, internet service providers and other online services to avoid liability for content posted by users and other third parties that qualifies as “online child sexual abuse material.”

While the national commission still includes the attorney general, secretary of Homeland Security, chairman of the Federal Trade Commission and 16 others chosen by Congress, compliance with the commission’s “best practices” will be voluntary and the states will be responsible for enforcing them.

The second change concerns the protections granted under what is known as Section 230 of the Telecommunications Act of 1996, which states, “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.” The original provisions of the EARN IT Act

required companies to “earn” their Section 230 protections. The bill approved by the committee removes entirely the “earn it” concept and opens tech companies up to criminal or civil charges against them by state governments.

Numerous tech and free speech experts and organizations immediately attacked the new legislation as a “bait and switch” which, far from improving upon the terms of the original draft presented by Graham and Blumenthal last March, intensifies its assault on free speech and electronic communications free from government surveillance.

Riana Pfefferkorn, associate director of surveillance and cybersecurity at the Stanford Center for Internet and Society, wrote that the EARN IT Act uses widespread resentment about Section 230 to stage an attack on encryption. “Encryption, particularly end-to-end encryption, is likely to be targeted as being contrary to ‘best practices’ for preventing [child sexual abuse material], because if a provider cannot ‘see’ the contents of files on its service due to encryption, it is harder to detect [child sexual abuse material] files.”

The Electronic Frontier Foundation wrote on July 2, “instead of giving a 19-person federal commission, dominated by law enforcement, the power to regulate the Internet, the bill now effectively gives that power to state legislatures. And instead of requiring that Internet websites and platforms comply with the commission’s ‘best practices’ in order to keep their vital legal protections under Section 230 for hosting user content, it simply blows a hole in those protections.”

In a comment on the passage of the redraft through the Senate committee, Graham said, “To those who shared the horrors of child sexual abuse on the internet with the Committee, you inspired us to act and you made it impossible for us to look away.” The bill is also

cosponsored by leading Democratic Senators Dianne Feinstein of California, Patrick Leahy of Vermont and Dick Durbin of Illinois.

A particularly significant role was played by Leahy, who introduced an amendment purportedly to address concerns about how the bill undermines encryption technologies. While Leahy's amendment prohibits holding companies liable because they use "end-to-end encryption, device encryption, or other encryption services," the bill encourages state lawmakers to look for ways to undermine end-to-end encryption, such as forcing messages to be scanned for content violations on a local device before they get encrypted and sent along to their recipient.

The unanimous support of leading Democrats and Republicans for the reactionary EARN IT legislation indicates that US political establishment is arriving at a consensus for establishing government control of online content and communications. As powerful contradictions intensify within capitalist society along with the expansion of the internet, mobile wireless devices and social media—utilized by a growing movement of the working class and young people from below—the ruling establishment is moving toward a regime of censorship and unfettered invasion of privacy.

In May, just as mass demonstrations were beginning to unfold across the country after the brutal murder of George Floyd by police in Minneapolis, Minnesota, President Donald Trump issued a threat to "close down" or "strongly regulate" the social media platforms by removing their Section 230 protections after Twitter placed "fact checking" flags on his tweets.

There are also the efforts of the US Justice Department and Attorney General William Barr to pursue a lawsuit against Google for alleged anti-trust violations—including an implicit threat to "break up" the Silicon Valley tech monopoly—as well as congressional legislation that will force consumer mobile device manufacturers such as Apple to build law enforcement back-door access into their data encryption products.

www.wsws.org/contact



To contact the WSWS and the
Socialist Equality Party visit: