

Bipartisan Senate Judiciary Committee introduces bill that censors online content and attacks encryption

Kevin Reed
17 March 2020

Leading members of the Senate Judiciary Committee formally introduced a bipartisan bill on March 5 that escalates US government censorship of online content and directly attacks encryption of electronic communications under the cover of fighting online child sexual abuse material (CSAM).

Senate Judiciary Committee Chairman Lindsey Graham (Republican of South Carolina), US Senators Richard Blumenthal (Democrat of Connecticut), Josh Hawley (Republican of Missouri) and Ranking Member Dianne Feinstein (Democrat of California) jointly introduced the Eliminating Abusive and Rampant Neglect of Interactive Technologies Act (EARN IT Act) that purports to “encourage the tech industry to take online child sexual exploitation seriously.”

The concept behind the law is that tech companies have to “earn” their protected immunity from prosecution for any illegal content published by users on their platforms by scanning and decrypting every message, image or post. Until now, online service providers were not responsible—under what are known as the Section 230 provisions of the Communications Decency Act of 1996—for anything users publish on websites, social media accounts or cloud servers.

In introducing the bill, Senator Graham said, “This bill is a major first step. For the first time, you will have to earn blanket liability protection when it comes to protecting minors.” Senator Blumenthal added, “Companies that fail to comport with basic standards that protect children from exploitation have betrayed the public trust granted them by this special exemption.”

While claiming to fight online CSAM and enlisting

the support of 70 organizations involved in stopping child sexual exploitation, the bill’s actual content shows that its ultimate purpose is an attack on fundamental democratic rights.

The law calls for the creation of a 19-member commission controlled by the attorney general and US law enforcement agencies. The EARN IT commission will establish “best practices” that must be followed by the technology companies or they will face criminal prosecution if content on their services is found to be illegal.

According to the Electronic Frontier Foundation (EFF), among the “best practices” of the EARN IT Act is a proposal by John Shehan, vice president at the National Center for Missing and Exploited Children (NCMEC), that says, “online services should be made to screen their messages for material that NCMEC considers abusive; use screening technology approved by NCMEC and law enforcement; report what they find in the messages to NCMEC; and be held legally responsible for the content of messages sent by others.”

Therefore, the EARN IT law will place the tech companies and their users in a Catch-22. The law mandates that tech providers either agree to monitor the content and violate the privacy and free speech rights of their users by screening everything they publish, post or store on the service or they agree to be prosecuted by the state for any illegal content that appears on their site.

EFF further explains that the 19-member commission will be “completely dominated by law enforcement and allied groups like NCMEC,” and “the bill gives Attorney General Barr the power to veto or approve the list of best practices. Even if other commission

members do disagree with law enforcement, Barr's veto power will put him in a position to strongarm them."

It is well known that William Barr and the US Justice Department have been advocates of online censorship and for abolishing end-to-end encryption in consumer electronic devices. There is nothing stopping the EARN IT Act from introducing as one of its "best practices" a provision for law enforcement's back-door access to encrypted communications and data files. Those firms which refuse to comply would then have their Section 230 protections eliminated.

It is a measure of the dishonesty of the American political system that leading Democrats and Republicans can so transparently use the fears and emotions of the public against child exploitation as a means of attacking fundamental rights protected by the Constitution.

On May 11, the Senate Judiciary Committee held a public hearing on the EARN IT Act and took testimony from witnesses on the proposed legislation. Among the speakers were representatives from the NCMEC, Jared Sine of the online dating company Match Group, a child exploitation legal expert, and Elizabeth Banker of the Internet Association. Of these speakers, only the last spoke against the EARN IT Act.

In her presentation, Banker explained that many of the major tech firms today—including Amazon, Ebay, Facebook, Google, Microsoft, Twitter and Uber—are members of the Internet Association. She went on to review the "multi-faceted" measures that tech companies have been engaged in to combat CSAM, going back to the passage of the Communications Decency Act of 1996, from their platforms.

Banker then explained how the EARN IT Act would "create numerous problems and hinder the efforts to combat CSAM" by violating online users' First and Fourth Amendment rights because the providers will be acting as "agents of the government." She stated, "Under Fourth Amendment jurisprudence, a search performed by an agent of the government is subject to the same requirements as if the government performed the search directly."

Banker also spoke about the implications for freedom of speech in the Senate Judiciary Committee bill, "The EARN IT Act would delegate important decisions concerning security, privacy, and free speech on the

internet—weighty and complex matters that directly impact hundreds of millions of consumers—to an administrative body that would be composed of members who are not elected representatives and that would operate with little transparency."

Finally, Banker said that although the bill does not specifically mention encryption, "Requiring companies to engineer vulnerabilities into their services would make us all less secure. Encryption technology stands between billions of internet users around the globe and innumerable threats—from attacks on sensitive infrastructure, including our highly automated financial systems, to attempts by repressive governments to censor dissent and violate human rights."

It could not have been lost on the Democratic and Republican senators or Elizabeth Banker of the Internet Association that the greatest threat of censorship and violation of human rights all over the world, including within the US itself, comes from American imperialism.



To contact the WSWS and the
Socialist Equality Party visit:

wsws.org/contact