

Bill targeting online child abuse puts encryption in crosshairs

March 8 2020, by Rob Lever



Major online services would be forced to do more to help fight online child exploitation or lose liability protection under a bill unveiled by senators and assailed by digital rights activists

A bill aimed at curbing online child sex abuse is pitting the US

government against the tech sector, in a battle about encryption and liability for illegal online content.

The bipartisan measure unveiled by US senators Thursday ties together two separate issues—law enforcement's access to encrypted online content, and tech platforms' [legal immunity](#) for what users post.

In unveiling the measure, senators said they were aiming to curb images of child sex abuse by forcing tech platforms to cooperate with law enforcement on encryption or risk losing the legal immunity for what is posted on their websites.

Digital rights activists have joined the [tech sector](#) in arguing this move is an indirect way to weaken online encryption in the name of better law enforcement access.

They say it erodes two cornerstones of the online ecosystem: strong encryption to keep data secure, and a liability shield which enables [social media platforms](#) to allow users to post content freely.

The bill "would give [government officials](#) unprecedented powers to craft de facto regulations for online speech," said Emma Llanso of the Center for Democracy and Technology, a digital rights organization.

"Online service providers would almost certainly err on the side of caution and take down anything—including a lot of lawful, constitutionally protected speech."



Republican US Senator Lindsey Graham (R) and Democratic Senator Richard Blumenthal (L) are sponsoring a bill that would force tech firms to do more to help fight child exploitation, which critics say would erode digital rights

'Kneecapping' encryption

Encryption has been a point of contention between tech firms and law enforcement for decades. FBI officials have warned of "going dark" in investigating crimes as a result of new forms of end-to-end encryption, while civil rights advocates warn that any "backdoor" access could be exploited by hackers and authoritarian governments.

The proposal "aims to kneecap encryption under the guise of protecting children online, while capitalizing on the techlash," said Riana

Pfefferkorn of the Stanford University Center for Internet and Society, referring to the simmering discontent with Big Tech over [data protection](#) and other issues.

Lawmakers say the bill—Eliminating Abusive and Rampant Neglect of Interactive Technologies Act (EARN IT)—allows companies to "earn" their liability protection, by gaining certification of compliance by a commission of government, industry, legal and victim group representatives.

A hearing is set for Wednesday on the measure, which is backed by victims' rights organizations.

They, along with the Justice Department, have complained that existing laws protecting platforms such as social media companies from liability for user-posted content have allowed child pornography and images of exploitation to proliferate.



US Attorney General Bill Barr has said encryption of data on phones and messaging apps makes it harder to catch criminals and thwart exploitation

'Shouldn't need a pass'

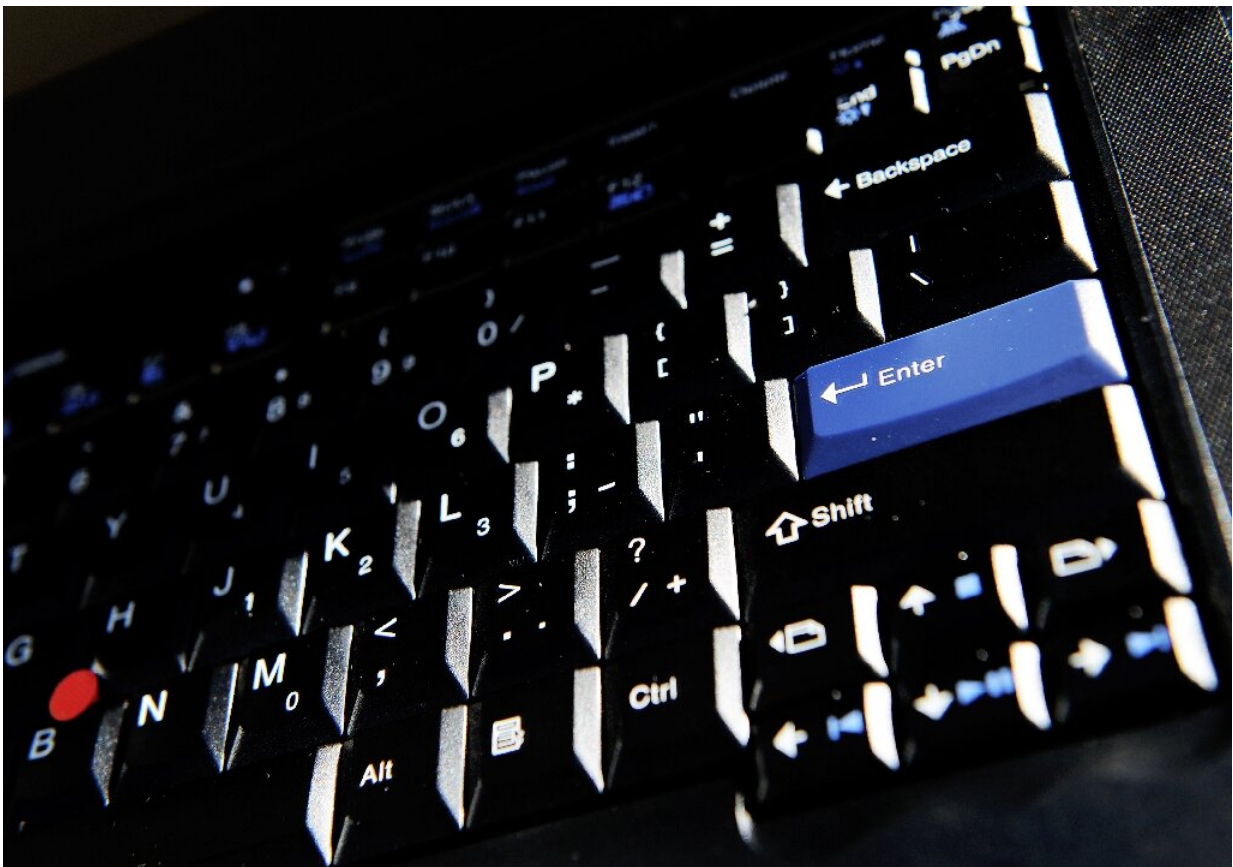
Critics say the bill, if enacted, could lead to draconian internet regulation.

"You shouldn't need to get a pass from a commission of [law enforcement](#) agencies just to set up a website," said Joe Mullin of the Electronic Frontier Foundation.

"That's the type of system we might hear about under an authoritarian regime."

Gary Shapiro, president of the Consumer Technology Association, a trade group including hundreds of online firms, said the bill "sets up the false choice between child safety and internet safety."

Shapiro said in a blog post that the proposed law would not stop the use of [encryption](#) but "penalize American companies by forcing those interested in secure communication to move their business to offshore companies not governed by US law."



Proposed US legislation aims to encourage firms to do more to curb the spread of content related to child sex abuse, but critics say it would do little

Full implications unclear

Eric Goldman, director of Santa Clara University's High Tech Law Institute, said authorities are already unable to investigate the vast number of potential sex exploitation cases flagged by tech firms.

"The core presumption of the bill is that companies aren't doing enough," Goldman said. "I don't think that's true. They treat this as the most toxic and most problematic kind of content."

The full implications of the bill remain unclear because standards would be set by a commission that would be created by lawmakers, Goldman said, adding that the panel could call for strict bans on encrypted apps or verification of the identity of all internet users, for example.

"There is no limit to the perniciousness of the recommendations," he said.

© 2020 AFP

Citation: Bill targeting online child abuse puts encryption in crosshairs (2020, March 8) retrieved 26 September 2023 from <https://techxplore.com/news/2020-03-bill-online-child-abuse-encryption.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.