The EARN IT Act Is a Sneak Attack on Encryption

Lily Hay Newman

March 5, 2020

A bipartisan pair of US senators today introduced long-rumored legislation known as the EARN IT Act. Meant to combat child sexual exploitation online, the bill threatens to erode established protections against holding tech companies responsible for what people do and say on their platforms. It also poses the most serious threat in years to strong end-to-end encryption.

As the final text of the bill circulated, the Department of Justice held a press conference about its own effort to curb online child predation: a set of 11 "voluntary principles" that a growing number of tech companies—including Facebook, Google, Microsoft, Roblox, Snap, and Twitter—have pledged to follow. Though the principles the companies are pledging to adopt don't specifically impact encryption themselves, the event had an explicit anti-encryption message. The cumulative effect of this morning's announcements could define the geography of the next crypto wars.

Child predators "communicate using virtually unbreakable encryption," US attorney general William Barr said during the press conference. "The department for one is prioritizing combatting child sexual exploitation and abuse in our prosecution efforts. And we are also addressing child exploitation in our efforts on retaining lawful access and in analyzing the impact of Section 230 of the Communications Decency Act on incentives for platforms to address these crimes."

EARN IT focuses specifically on Section 230, which has historically given tech companies freedom to expand with minimal liability for how people use their platforms. Under EARN IT, those companies wouldn't automatically have a liability exemption for activity and content related to child sexual exploitation. Instead, companies would have to "earn" the protection by showing that they are following recommendations for combatting child sexual exploitation laid out by a 16-person commission.

"This is a profoundly awful proposal on multiple levels."

JULIAN SANCHEZ, CATO INSTITUTE

The bill, written by South Carolina Republican senator Lindsey Graham and Connecticut Democrat Richard Blumenthal, would create a way for law enforcement officials, attorneys general, online child sexual exploitation survivors and advocates, constitutional law scholars, consumer protection and privacy specialists, cryptographers, and other tech experts to collectively decide what digital companies should do to identify and reduce child predation on their platforms—and then require companies to actually do it. The safeguards the committee

might recommend would likely include things like proactive, dynamic content scanning to identify abusive photos and videos, but also communication surveillance to watch for predators who could be forming relationships with potential victims and "grooming" them for exploitation.

Though it seems wholly focused on reducing child exploitation, the EARN IT Act has definite implications for encryption. If it became law, companies might not be able to earn their liability exemption while offering end-to-end encrypted services. This would put them in the position of either having to accept liability, undermine the protection of end-to-end encryption by adding a backdoor for law enforcement access, or avoid end-to-end encryption altogether.

Facebook has most prominently made the argument in recent months that it can adequately identify child predation threats without eliminating or undermining user data protections like end-to-end encryption. The safeguard only makes data readable on the sender's and receiver's devices, boxing companies out of accessing user data directly.

Law enforcement officials and members of Congress have countered, though, that tech companies can't do enough to stop child predation and distribution of illegal content on their platforms if they can't access their users' data.

"We share the EARN IT Act sponsors' commitment to child safety and have made keeping children safe online a top priority by developing and deploying technology to thwart the sharing of child abuse material," Thomas Richards, a Facebook spokesperson, said in a statement. "We're concerned the EARN IT Act may be used to roll back encryption, which protects everyone's safety from hackers and criminals, and may limit the ability of American companies to provide the private and secure services that people expect."