tech.co

Why the EARN IT Act Is Bad News for Data Encryption

Adam Rowe

March 11th 2020

Congress introduced the EARN IT act last week – a bipartisan measure, aimed at stopping child sex abuse online. But, many tech experts are warning that it will only serve to erode the encryption standards that ward off mass government surveillance.

It's just the latest illustration that data privacy can be tough to regulate. Or, at least, tough for the US Congress.

We explain all you need to know about the EARN IT act, including why it's received such a frosty reception.

What the EARN IT Act seeks to tackle

The bill was put forward by two senators: South Carolina Republican Lindsey Graham and Connecticut Democrat Richard Blumenthal. The EARN IT title is short for “Eliminating Abusive and Rampant Neglect of Interactive Technologies,” because all bills need cool acronyms.

Currently, big social media messaging services such as iMessage, WhatsApp, Telegram and Facebook Messenger keep their users' messages and data encrypted. The government can get access on some occasions, but only in situations that justify getting a warrant. Though there has been some notable cooperation, big tech companies have largely been resistant to letting government of law enforcement get sight of encrypted data. Indeed, services such as Telegram proudly promote themselves as bastions of data privacy for users.

Under the EARN IT act, though, the government would revoke a form of liability currently granted by Section 230 of the Communications Decency Act. If EARN IT passes, these messaging platforms would be liable for any child abuse materials found on their platform. This would give these platforms a huge incentive to surveil the data in order to ensure they don't face penalties.

Why the EARN IT Act may be a bad idea

The new regulation doesn't directly remove encryption, nor directly expose users' data. But, it does shift the burden of avoiding legal action onto the social platforms and messaging services themselves. This move gives those platforms a big incentive to undermine their own end-to-end encryption efforts, either by adding a backdoor that gives government access to user data, or by otherwise loosening their encryption.

On top of that, the act gives government powers another in-road toward mass surveillance — even on matters unrelated to child exploitation.

“Looking at the additional language, it’s clear to me that this is still going to be a vehicle for the attorney general to wage his war on encryption. And it's kind of a black box,” Riana Pfefferkorn, associate director of surveillance and cybersecurity at Stanford's Center for Internet and Society, told Wired. “One of my fears is if this were implemented, what’s to stop China from saying ‘in addition to monitoring for child sex abuse images, turn this on for Uighur freedom activists too.'”

Other experts held even stronger opinions, with the Cato Institute's Julian Sanchez calling it a “profoundly awful proposal on multiple levels,” and Matthew Green of Johns Hopkins University terming it a “sophisticated and direct governmental attack on the right of Americans to communicate privately.”

Child sexual exploitation online is a serious issue. But it's important to examine any potential fallout of regulation intended to address it. After all, this wouldn't be the first time the US government has faced poor consequences after attempting to address sexual exploitation through new bipartisan regulations.

Why Congress doesn't “get” the internet

You can't regulate an industry you don't understand, and US lawmakers have a spotty track record when it comes to understanding the worlds of tech and social media.

Tim Cook himself has called dealing with a tech-illiterate Congress “a challenge.” Famously, when Mark Zuckerberg subjected himself to a congressional hearing, he dealt with questions as basic as, “How do you sustain a business model when people don’t pay for services?” and “Is Twitter the same as what you do?” That last question was from Senator Lindsay Graham — the same guy behind the EARN IT Act itself.

It's wrongly tempting to blame the government overseers' lack of tech savvy on their demographic, given that the average senator is 61 years old. But the real issue is likely the total lack of crossover between congressional knowledge and real-world technology experience.

What's in the future? More regulation

The US government is in (rare!) bipartisan agreement on one thing: better internet privacy laws are needed nationwide. A national law will likely happen in the near future, too, according to many expert opinions.

Last year, the Federal Trade Commission recommended Congress introduce a federal privacy law in order to protect user data. It's likely we'll see one soon, and it's pretty easy to point out the need for better regulation. A good policy would stave off incidents like Cambridge Analytica's early 2018 Facebook data-mining scandal.

But, would it be a good policy? The valid criticisms of the new EARN IT act make one thing clear. For all its good intentions, Congress still hasn't convinced those it serves that it can create effective internet regulation.