September 15, 2020

United States Senate

Re: **Opposition to the *Eliminating Abusive and Rampant Neglect of Interactive Technologies Act of 2020* (EARN IT Act)**

Dear Senator:

The undersigned organizations write to express our strong opposition to the *Eliminating Abusive and Rampant Neglect of Interactive Technologies Act of 2020* (EARN IT, S.3398). We support curbing the scourge of child exploitation online. However, EARN IT will result in online censorship that will disproportionately impact marginalized communities, will jeopardize access to encrypted services, and will place at risk the prosecutions of the very abusers the law is meant to catch. We urge you **to object to any motion for unanimous consent to place the bill on the Senate floor and to vote NO on passage of the bill in its current form**.

Section 230 of the Communications Act of 1934 (as amended, 47 U.S.C. § 230) generally shields online intermediaries from liability for the content users convey on their platforms. This promotes free expression and allows for the use of robust end-to-end encryption. Section 230 has never been a bar to federal criminal prosecution of intermediaries and current law imposes federal criminal liability on service providers who have knowledge that they are distributing child sexual abuse material (CSAM).[1] And current law requiring providers to report these images results in millions of reports to the National Center for Missing and Exploited Children every year.[2] EARN IT would vastly expand the liability risk of hosting or facilitating user-generated content by permitting states to impose criminal liability when providers are "reckless" or "negligent" in keeping CSAM off their platforms; EARN IT also exposes them to civil liability under state law. This change will threaten our ability to speak freely and securely online, and threaten the very prosecutions the bill seeks to enable.

The EARN IT Act Threatens Free Expression

EARN IT would repeal platforms' Section 230 liability shield for any state criminal and civil law prohibiting CSAM distribution.[3] EARN IT places no *mens rea* limitation on these laws, which means states will be free to impose any liability standard they please on platforms, including holding platforms liable for CSAM they did not actually know was present on their services. Nothing in the bill would prevent a state from passing a law in the future holding a provider criminally responsible under a "reckless" or "negligence" standard. At least one state, Florida, already imposes a lower standard for liability on CSAM distribution than the federal standard,

[1] 18 U.S.C. § 2252.
[2] National Center for Missing and Exploited Children, NCMEC Data (last visited Aug. 24, 2020), https://www.missingkids.org/ourwork/ncmecdata (16.9 million reports to the Cyber TipLine in 2019).
[3] Indeed, EARN IT opens providers up to lawsuits and criminal charges beyond distribution of CSAM. The bill would permit liability for state criminal and civil law "regarding the advertisement, promotion, presentation, distribution, or solicitation of child sexual abuse material" as defined in federal law with disastrous consequences. *See* Ben Horton, *EARN It's State-law Exemption Would Create Bewildering Set of Conflicting Standards for Online Speech*, Center for Democracy & Technology (Aug. 11, 2020), https://cdt.org/insights/earn-its-state-law-exemption-would-create-bewildering-set-of-conflicting-standards-for-online-speech.

allowing liability for distributors that did not have actual knowledge.[4] By opening providers up to significantly expanded liability, the bill would make it far riskier for platforms to host user-generated content. Providers facing potential liability under dozens of laws regulating conduct at different standards may simply choose to forgo hosting user content. For those who forge on, in order to mitigate the legal risks inherent in the massive expansion of liability imposed by EARN IT, providers will engage in overbroad censorship that will burden online speech, especially content created by diverse communities, including LGBTQ individuals, and content carried on platforms ranging from social media apps to video game websites designed for minors and young adults.[5]

Looking to the past as prelude to the future, the only time that Congress has limited Section 230 protections was in the Allow States and Victims to Fight Online Sex Trafficking Act (SESTA/FOSTA). That law purported to protect victims of sex trafficking by eliminating providers' Section 230 liability shield for "facilitating" sex trafficking by users. Instead, it has forced sex workers, whether voluntarily engaging in sex work or forced into sex trafficking against their wills, offline and into harm's way. It has also chilled their online expression generally, including the sharing of health and safety information, and speech wholly unrelated to sex work. Moreover, these burdens fell most heavily on smaller platforms that either served as allies and created spaces for the LGBTQ and sex worker communities or simply could not withstand the legal risks and compliance costs of SESTA/FOSTA.[6] Congress risks repeating this mistake by rushing to pass this misguided legislation, which also limits Section 230 protections.

The EARN It Act Jeopardizes the Security of Our Communications

End-to-end encryption ensures the privacy and security of sensitive communications such that only the sender and receiver can view them. This security is relied upon by journalists,[7] Congress,[8] the military,[9] domestic violence survivors,[10] and anyone who seeks to keep their

---

[4] Florida §847.0137 broadly criminalizes the transmission of CSAM ("any person in this state who knew or reasonably should have known that he or she was transmitting child pornography…").
[5] Ben Horton, *EARN It's State-law Exemption Would Create Bewildering Set of Conflicting Standards for Online Speech*, Center for Democracy & Technology (Aug. 11, 2020), https://cdt.org/insights/earn-its-state-law-exemption-would-create-bewildering-set-of-conflicting-standards-for-online-speech/.
[6] *See* Danielle Blunt and Ariel Wolf, *Erased The Impact of FOSTA-SESTA*, Hacking//Hustling (2020), https://hackinghustling.org/wp-content/uploads/2020/01/HackingHustling-Erased.pdf; Makena Kelly, *Democrats want data on how sex workers were hurt by online crackdown*, The Verge (Dec. 17, 2019), https://www.theverge.com/2019/12/17/21026787/sesta-fosta-congress-study-hhs-sex-work-ro-khanna-elizabeth-warren-ron-wyden.
[7] Internet Society & Committee To Protect Journalists, *Encryption How It Can Protect Journalists and the Free Press*, ISOC (March 2020), https://www.internetsociety.org/wp-content/uploads/2020/03/Encryption-for-Journalists-Factsheet.pdf.
[8] Zach Whittaker, *In encryption push, Senate staff can now use Signal for secure messaging*, ZDNet (May 16, 2017), https://www.zdnet.com/article/in-encryption-push-senate-approves-signal-for-encrypted-messaging/.
[9] Shawn Snow, Kyle Rempfer & Meghann Myers, *Deployed 82nd Airborne unit told to use these encrypted messaging apps on government cell phones*, The Military Times (Jan. 23, 2020), https://www.militarytimes.com/flashpoints/2020/01/23/deployed-82nd-airborne-unit-told-to-use-these-encrypted-messaging-apps-on-government-cellphones/.
[10] Kaitlyn Well & Thorin Klosowski, *Domestic Abusers Can Control Your Devices. Here's How to Fight Back*, N.Y. Times Wirecutter (Apr. 6, 2020), https://www.nytimes.com/wirecutter/blog/domestic-abusers-can-control-your-devices-heres-how-to-fight-back/.

communications secure from malicious hackers. But the EARN IT Act threatens to undermine and disincentivize providers from providing strong encryption. The Senate Judiciary Committee adopted an amendment to EARN IT specifying that providers will not be responsible for violating CSAM laws "because" they offer encrypted services. While we support the goal of the amendment, it fails to fully resolve the encryption concerns with the bill. As amended, the bill invites repeated and protracted litigation about whether a provider's decision to provide encrypted services was the entire cause for its failure to adopt certain practices to combat CSAM. For example, the amendment does not clearly protect providers against liability if they do not comply with mandates to employ certain techniques that are incompatible with secure end-to-end encryption. Techniques such as client-side scanning and sender authentication can give law enforcement access to communications content. But, each technique undermines the promise of end-to-end encryption—that only the sender and recipient will be able to understand the content of the communication. Use of such techniques would be incompatible with a secure end-to-end encrypted service. Whether courts agree that forgoing implementation of such measures fits under the encryption umbrella would become a subject of protracted litigation.

Additionally, EARN IT sets up a law enforcement-heavy and Attorney General-led commission charged with producing a list of voluntary best practices that providers should adopt to address CSAM on their services. The Commission is free to, and likely will, recommend against the offering of end-to-end encryption, and recommend providers adopt techniques that weaken the cybersecurity of their product. While these best practices would be voluntary, they could result in reputational harm to providers if they choose not to comply, and inform how judges evaluate a provider's liability. States may even amend their laws to mandate the adoption of these best practices. For many companies, the lack of clarity and fear of liability, in addition to potential public shaming, will likely disincentivize them from offering strong encryption, at a time when we should be doing the opposite.

The EARN IT Act Risks Undermining Child Abuse Prosecutions

The EARN IT Act risks transforming providers into agents of the government for purposes of the Fourth Amendment.[11] If a state law has the effect of compelling providers to monitor or filter their user's content so it can be turned over to the government for criminal prosecution, the provider becomes an agent of the government and any CSAM it finds could become the fruit of an unconstitutional warrantless search.[12] In that case, the CSAM would properly be suppressed as evidence in a prosecution and the purveyor of it could go free. At least two state laws—those of Illinois and South Carolina—would have that effect.[13]

---

[11] Hannah Quay-de la Vallee & Mana Azarmi, *The New EARN IT Act Still Threatens Encryption and Child Exploitation Prosecutions*, Center for Democracy & Technology (Aug. 25, 2020), https://cdt.org/insights/the-new-earn-it-act-still-threatens-encryption-and-child-exploitation-prosecutions/.

[12] *See Skinner v. Railway Labor Executives' Association*, 489 U.S. 602, 614 (1989) ("Although the Fourth Amendment does not apply to a search or seizure, even an arbitrary one, effected by a private party on his own initiative, the Amendment protects against such intrusions if the private party acted as an instrument or agent of the Government."). *See also*, *United States v. Stevenson*, 727 F.3d 826, 829 (8th Cir. 2013) ("Even when a search is not required by law, however, if a statute or regulation so strongly encourages a private party to conduct a search that the search is not 'primarily the result of private initiative,' then the Fourth Amendment applies").

[13] Illinois 720 ILCS 5/11-20 (2012) (this law compels providers to inspect the contents of their customer's communications for CSAM in violation of the Fourth Amendment); South Carolina SC Code § 16-15-305 (2012)

***

The EARN IT Act would have devastating consequences for our ability to share and access information online, and to do so in a secure manner. We urge you to oppose this bill. Congress should instead consider more tailored approaches to deal with the real harms of CSAM online. Please direct any questions about this letter to the Center for Democracy & Technology's Emma Llansó, Director of the Free Expression Project at ellanso@cdt.org or Greg Nojeim, Director of the Freedom, Security & Technology Project at gnojeim@cdt.org.

Sincerely,

Access Now
Advocacy for Principled Action in Government
American Civil Liberties Union
ARTICLE 19
Canadian Civil Liberties Association
Center for Democracy & Technology
Center for Technology and Society of the University of San Andres
Copia Institute
Demand Progress
Derechos Digitales
Electronic Frontier Foundation
Fight for the Future
Free Press Action
Freedom to Read Foundation
Internet Society
LGBT Tech
National Coalition Against Censorship
New America's Open Technology Institute
OpenMedia
Prostasia Foundation
R Street Institute
S.T.O.P. - The Surveillance Technology Oversight Project
The Tully Center for Free Speech
Wikimedia Foundation
Woodhull Freedom Foundation
X-Lab

(the *mens rea*, or level of knowledge that triggers liability is so low that any encrypted service could face criminal liability).