February 9, 2022

Chairman Dick Durbin
Committee on the Judiciary
United States Senate
711 Hart Senate Building
Washington, D.C. 20510

Ranking Member Chuck Grassley
Committee on the Judiciary
United States Senate
135 Hart Senate Office Building
Washington, DC 20510

Re: Opposition to the Eliminating Abusive and Rampant Neglect of Interactive Technologies Act of 2022 (EARN IT Act)

Dear Chairman Durbin, Ranking Member Grassley, and members of the Committee:

The undersigned organizations write to express our strong opposition to the Eliminating Abusive and Rampant Neglect of Interactive Technologies Act of 2022 (EARN IT, S.3538). We support curbing the scourge of child exploitation online. However, EARN IT will actually make it harder for law enforcement to protect children. It will also result in online censorship that will disproportionately impact marginalized communities and will jeopardize access to encrypted services. Dozens of organizations and experts[1] warned this committee of these risks when this bill was previously considered, and all of those same risks remain. We urge you **to oppose this bill.**

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 helps to promote free expression online, which is further supported by the use of strong end-to-end encryption. Section 230 has never been a bar to federal criminal prosecution of intermediaries and current federal law imposes criminal liability on service providers who have knowledge that they are distributing child sexual abuse material (CSAM).[2] 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.[3] EARN IT would vastly expand the liability risk of hosting or facilitating user-generated content by permitting states to impose

[1] *See* Letter from TechFreedom et al. (Sept. 30, 2020), https://techfreedom.org/wp-content/uploads/2020/09/EARN-IT-Coalition-Letter-9.30.2020.pdf; Letter from AccessNow et al. (Sept. 15, 2020), https://cdt.org/wp-content/uploads/2020/09/Civil-Society-Coalition-Letter-EARN-IT-Act-9.15.20.pdf; Letter from Advocates for Youth, et al. (Sept. 9, 2020), https://freedomnetworkusa.org/app/uploads/2020/09/FNUSA-Joins-EARN-IT-Act-Coalition-letter- 9.09.2020.pdf; Coalition Letter on EARN IT Act (July 2, 2020), https://rstreet.org/2020/07/02/coalition-letter-on- earn-it-act/ ; ACLU Letter Of Opposition to EARN IT Act Manager's Amendment (July 1, 2020), https://www.aclu.org/letter/aclu-letter-opposition-earn-it-act-managers-amendment; EFF Letter of Opposition to EARN IT Markup (July 1, 2020), https://www.eff.org/document/eff-letter-opposition-earn-it-markup; Letter to US Senate Judiciary Committee: Reject the EARN IT Act, S. 3398 (June 1, 2020), https://www.hrw.org/news/2020/06/01/letter-us-senate-judiciary-committee-reject-earn-it-act-s-3398.

[2] 18 U.S.C. § 2252.

[3] National Center for Missing and Exploited Children, NCMEC Data (last visited Feb. 3, 2022), https://www.missingkids.org/ourwork/ncmecdata (21.7 million reports to the Cyber TipLine in 2022).

criminal liability when providers are "reckless" or "negligent" in keeping CSAM off their platforms; EARN IT also exposes them to civil liability under state laws with similar mens rea requirements but subject to much lower standards of proof. These changes 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 the "distribution" or "presentation" of CSAM.[4] 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.[5] 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, allowing liability for distributors that did not have actual knowledge.[6] By opening providers up to significantly expanded liability, the bill would make it far riskier for platforms to host user-generated content. Facing potential liability under dozens of laws regulating conduct at different standards, providers 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 under state law enabled by EARN IT, providers will engage in overbroad censorship of online speech, especially content created by diverse communities, including LGBTQ individuals, whose posts are disproportionately labeled erroneously as sexually explicit,[7] and content carried on platforms ranging from social media apps to video game websites designed for minors and young adults.[8]

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 of 2017 (SESTA/FOSTA). That law purported to protect victims of sex trafficking by eliminating providers' Section 230 liability shield for "facilitating" sex trafficking by users. According to a 2021 study by the US Government Accountability Office, however, the law has been rarely used to combat sex trafficking.[9]

---

[4] 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.

[5] EARN IT would allow state laws to hold services liable for user content even when it cannot be shown that they should have known of specific content (constructive knowledge). Recklessness is an even lower standard, requiring only that a defendant consciously disregarded a substantial and unjustified risk.

[6] Florida law broadly criminalizes the transmission of CSAM. Fla. Stat. § 847.0137(2) (stating that "any person in this state who knew or reasonably should have known that he or she was transmitting child pornography...commits a felony of the third degree").

[7] John Hudson, The Controversy Over Facebook's Gay Kissing Ban Isn't Over, The Atlantic (Apr. 22, 2011), https://www.theatlantic.com/technology/archive/2011/04/controversy-over-facebooks-gay-kissing-ban-isnt-over/349921/; Harry Readhead, Facebook criticised for removing lesbian kiss photo posted to mark anti-homophobia day, Metro (May 20, 2014), https://metro.co.uk/2014/05/20/facebook-criticised-for-removing-lesbian-kiss-posted-to-mark-anti-homophobia-day-4733954/.

[8] Ben Horton, *supra* n.4.

[9] Government Accountability Office. (2021). Sex Trafficking: Online Platforms and Federal Prosecutions. (GAO Publication No. 21-385), https://www.gao.gov/assets/gao-21-385.pdf (reporting that the Department of Justice had brought just one case under FOSTA, which at the time of the report remained in court with no restitution sought, and that only one individual had pursued civil damages, in a case that was dismissed).

Instead, it has forced sex workers, whether voluntarily engaging in sex work or forced into sex trafficking against their will, offline and into harm's way.[10] It has also chilled their online expression generally, including the sharing of health and safety information, and speech wholly unrelated to sex work.[11] 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.[12] 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,[13] Congress,[14] the military,[15] domestic violence survivors,[16] union organizers,[17] and anyone who seeks to keep their communications secure from malicious hackers. Everyone who communicates with others on the internet should be able to do so privately. But by opening the door to sweeping liability under state laws, the EARN IT Act would strongly disincentivize providers from providing strong encryption. Section 5(7)(A) of EARN IT states that provision of encrypted services shall not "serve as an independent basis for liability of a provider" under the expanded set of state criminal and civil laws for which providers would face liability under EARN IT. Further, Section 5(7)(B) specifies that courts will remain able to consider information about whether and how a provider employs end-to-end encryption as evidence in cases brought under EARN IT. This language, originally proposed in last session's House

---

[10] See Online Platforms and Sex Worker Discrimination, Hacking//Hustling (last visited Feb. 3, 2022), https://hackinghustling.org/online-platforms-sex-worker-discrimination/ (continuously updated document listing companies, institutions, and products "that in some way discriminate or ban sex work or adult products OR have been shut down completely following increased anti-sex work legislation"); LaLa B Holston-Zannell, PayPal and Venmo are Shutting Out Sex Workers, Putting Lives and Livelihoods at Risk, ACLU (June 23, 2021), https://www.aclu.org/news/lgbtq-rights/paypal-and-venmo-are-shutting-out-sex-workers-putting-lives-and-livelihoods-at-risk/.

[11] See, e.g., Amanda Waltz, Sex workers in Pittsburgh discuss local impact of damaging anti-trafficking law FOSTA-SESTA, Pittsburgh City Paper (Apr. 7, 2021), https://www.pghcitypaper.com/pittsburgh/sex-workers-in-pittsburgh-discuss-local-impact-of-damaging-anti-trafficking-law-fosta-sesta/Content?oid=19226930 (quoting a researcher at the University of Pittsburgh describing how SESTA/FOSTA has led platforms to suppress the political speech of sex workers, including online organizing efforts); Jessica Stoya, What We Can Really Learn From the OnlyFans Debacle, Slate (Aug. 25, 2021), https://slate.com/human-interest/2021/08/onlyfans-sex-banned-allowed-decision-history.html (describing how SESTA/FOSTA led platforms to "decimate" online sex worker spaces—"from bad-date lists that providers use to warn one another about dangerous clients to Instagram hashtags where we'd organized to fight the very law causing these problems").

[12] 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.

[13] Internet Society & Committee To Protect Journalists, Encryption How It Can Protect Journalists and the Free Press, ISOC (Mar. 2020), https://www.internetsociety.org/wp-content/uploads/2020/03/Encryption-for-Journalists-Factsheet.pdf.

[14] 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/.

[15] 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/.

[16] 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/.

[17] Lorenzo Franceschi-Bicchierai & Lauren Kaori Gurley, How to Organize Your Workplace Without Getting Caught, Vice Motherboard (Jan. 15, 2020) https://www.vice.com/en/article/y3md3v/how-to-organize-your-workplace-without-getting-caught.

companion bill,[18] takes the form of a protection for encryption, but in practice it will do the opposite: courts *could* consider the offering of end-to-end encrypted services as evidence to prove that a provider is complicit in child exploitation crimes. While prosecutors and plaintiffs could not claim that providing encryption, alone, was enough to constitute a violation of state CSAM laws, they would be able to point to the use of encryption as evidence in support of claims that providers were acting recklessly or negligently. Even the mere threat that use of encryption could be used as evidence against a provider in a criminal prosecution will serve as a strong disincentive to deploying encrypted services in the first place.

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 ultimately weaken the cybersecurity of their products. While these "best practices" would be voluntary, they could result in reputational harm to providers if they choose not to comply. There is also a risk that refusal to comply could be considered as evidence in support of a provider's liability, and inform how judges evaluate these cases. States may even amend their laws to mandate the adoption of these supposed 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 encouraging 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.[19] If a state law has the effect of compelling providers to monitor or filter their users' 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.[20] 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.[21]

***

The EARN IT Act would have devastating consequences for everyone's ability to share and access

[18] H.R. 8454, 116th Cong. (EARN IT Act of 2020), https://www.congress.gov/bill/116th-congress/house-bill/8454/text; see also Riana Pfefferkorn, House Introduces EARN IT Act Companion Bill, Somehow Manages to Make It Even Worse (Oct. 5, 2020), https://cyberlaw.stanford.edu/blog/2020/10/house-introduces-earn-it-act-companion-bill-somehow-manages-make-it-even-worse

[19] 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/.

[20] 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").

[21] 720 ILCS 5/11-20 (2012) (Illinois law effectively compelling providers to inspect the contents of their customer's communications for obscenity, which would include CSAM, by criminalizing publication of obscenity with knowledge or after "recklessly failing to exercise reasonable inspection"); SC Code § 16-15-305 (2012) (South Carolina law effectively compelling providers to inspect the contents of their customer's communications for obscenity, which would include CSAM, by criminalizing "knowingly" disseminating obscenity and defining "knowingly" to include failing to exercise reasonable inspection).

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
Advocating Opportunity
American Civil Liberties Union
American Library Association
ARTICLE 19
Aspiration
Black and Pink
Black and Pink Massachusetts
Center for Democracy & Technology
Chicago House & Social Service Agency
Collaboration on International ICT Policy in East and Southern Africa (CIPESA)
Copia Institute
Defending Rights & Dissent
Due Process Institute
Electronic Frontier Foundation
Fight for the Future
Free Press Action
Free Speech Coalition
Freedom Network USA
Freedom to Read Foundation
GLAAD
Global Partners Digital
Global Voices
Human Rights Campaign
Institute for Local Self-Reliance
Internet Society
ISOC India, Hyderabad Chapter
JCA-NET (Japan)
Law and Technology Research Institute of Recife (IP.rec)
LGBT Technology Partnership
Media Alliance
Mnemonic
Mozilla Foundation
National Center for Lesbian Rights
National Center for Transgender Equality
National Coalition Against Censorship
New America's Open Technology Institute
Oakland Privacy
Old Pros
OpenMedia
PEN America
Privacy and Access Council of Canada
Progressive Technology Project
Public Knowledge
R3D: Red en Defensa de los Derechos Digitales
Ranking Digital Rights
Reframe Health and Justice
Restore the Fourth
S.T.O.P. – The Surveillance Technology Oversight Project
The Sex Workers Project of the Urban Justice Center
Society of Professional Journalists
Software Freedom Law Center, New York
SWOP Behind Bars
Tech for Good Asia
TechFreedom
Tutanota
Wikimedia Foundation
Woodhull Freedom Foundation
X-Lab
Youth Forum for Social Justice