May 2, 2023

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

Ranking Member Lindsey Graham
Committee on the Judiciary
United States Senate
211 Russell Senate Office Building
Washington, DC 20510

Re: Opposition to the Eliminating Abusive and Rampant Neglect of Interactive Technologies Act of 2023 (EARN IT Act)

Dear Chairman Durbin, Ranking Member Graham, 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 2023 (EARN IT, S.1207). We support curbing the scourge of child exploitation online. However, EARN IT will instead make it harder for law enforcement to protect children. It will also result in online censorship that will disproportionately impact marginalized communities. In addition, EARN IT will jeopardize access to encrypted services, undermining a critical foundation of security, confidentiality, and safety on the internet. Dozens of organizations and experts[1] have repeatedly warned this committee of these risks when this bill has been previously considered, and 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 services. Section 230's liability shield applies to smaller and start-up companies that are interactive computer service providers, not just a handful of large companies like Google and Meta. In addition, it protects both consumer-facing intermediaries like social media companies and infrastructure intermediaries that are crucial to running the internet and are not aware of the content that flows through their systems. Since its enactment, Section 230 has fueled innovation online, allowing millions of U.S.-based internet intermediaries to emerge over

[1] *See* Letter from Access Now et al. (Feb. 9, 2022); Riana Pfefferkorn, *The EARN IT Act is Back, and It's More Dangerous Than Ever*, Center for Internet and Society, (Feb. 4, 2022); Lisa Macpherson & John Bergmayer, *Is the new EARN IT Act "new wine in an old bottle"? Whatever it is, we're not buying it.*, Public Knowledge (Mar. 21, 2022); Joe Mullin, *It's Back: Senators Want EARN IT Bill to Scan All Online Messages*, Electronic Frontier Foundation (Feb. 3, 2022); Letter from TechFreedom et al. (Sept. 30, 2020); Letter from AccessNow et al. (Sept. 15, 2020); Letter from Advocates for Youth, et al. (Sept. 9, 2020); Coalition Letter on EARN IT Act (July 2, 2020); ACLU Letter Of Opposition to EARN IT Act Manager's Amendment (July 1, 2020); EFF Letter of Opposition to EARN IT Markup (July 1, 2020); Letter to US Senate Judiciary Committee: Reject the EARN IT Act, S. 3398 (June 1, 2020).

the last few decades. Section 230 also 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 intermediaries who have knowledge that they are distributing child sexual abuse material (CSAM).[2] Current law also requires intermediaries to report these images, resulting 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 criminal liability when intermediaries are "reckless" or "negligent" in keeping CSAM off their platforms; EARN IT also exposes them to civil liability under state laws with similar requirements with respect to the provider's mental state 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 intermediaries' Section 230 liability shield for any state criminal and civil law prohibiting the "distribution" or "presentation" of CSAM.[4] EARN IT requires no specific or minimum *mens rea* for state 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 that they were transmitting CSAM.[6]

By opening providers up to significantly expanded liability, the bill would make it far riskier for platforms to host user-generated content. Some states may conclude that an intermediary acted recklessly or negligently, for example, if it knows that its service has been used to convey CSAM in the past and it fails to proactively filter content. Such a standard would threaten free expression for online services that host user-generated content directly, because it would almost certainly cause them to remove constitutionally

---

[2] 18 U.S.C. § 2252.

[3] National Center for Missing and Exploited Children, *CyberTipline 2021 Report* (last visited May 1, 2023) (reporting that NCMEC received 32 million reports to the Cyber TipLine in 2022 and that more than 99.5% of the reports regarded incidents of suspected CSAM).

[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).

[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). States could hold services liable under a recklessness standard, i.e., proof that they consciously disregard a substantial and unjustified risk that it is distributing CSAM, *see* Black's Law Dictionary 1298 (8th Ed. 2004), or negligence, i.e. proof that a provider failed to exercise reasonable care, *see id.* 1061. In contrast, federal criminal law permits an intermediary to be held liable only if it has actual knowledge that it is distributing CSAM. 18 U.S.C. § 2252.

[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").

protected speech that is not CSAM. It would be particularly problematic for internet infrastructure intermediaries like content delivery networks and internet service providers, which are not designed nor meant to assess the content of the traffic they are carrying or helping to transport.[7]

Facing potential liability under dozens of laws regulating conduct at different standards, some intermediaries may choose to simply forgo hosting user content. Others will try to mitigate the legal risks inherent in the massive expansion of liability under state law enabled by EARN IT by engaging in overbroad censorship of online speech. These providers will remove any content that they suspect could be CSAM or even simply all sexually explicit content, sweeping up large amounts of content that are not CSAM and are constitutionally protected speech. These wide ranging removals of online speech will negatively impact diverse communities in particular, including LGBTQ people, whose posts are disproportionately labeled erroneously as sexually explicit.[8] As a result, LGBTQ people will be less free to express themselves online and less able to use the internet to find community[9] or to organize against anti-LGBTQ legislation and sentiments.[10] Overbroad removals of online speech will also especially impact content carried on platforms ranging from social media apps to video game websites designed for minors and young adults.[11]

Past experience demonstrates that these risks to online free expression are not hypothetical. The only time that Congress has limited Section 230 protections so far 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.[12] 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.[13] It has also chilled their online expression, including through platforms' overbroad removals of speech sharing health and safety information and speech wholly unrelated to sex work.[14] Moreover, these burdens have fallen

---

[7] Similar to postal and telephone services, infrastructure intermediaries make up the framework needed for data to flow. They do not create the data and should remain unaware of content flowing through their service.

[8] John Hudson, *The Controversy Over Facebook's Gay Kissing Ban Isn't Over*, The Atlantic (Apr. 22, 2011); Harry Readhead, *Facebook criticised for removing lesbian kiss photo posted to mark anti-homophobia day*, Metro (May 20, 2014).

[9] Amber Leventry, *The importance of social media when it comes to LGBTQ kids feeling seen*, Wash. Post (Sept. 19, 2019).

[10] HRC Staff, *Human Rights Campaign Slams Governor Lee for Signing Anti-Drag Bill and Gender Affirming Care Ban into Law; TN Becomes First State to Criminalize Drag*, Human Rights Campaign (Mar. 2, 2023); Change.org, *Transgender Rights* (last visited May 1, 2023).

[11] Horton, *supra* n.4.

[12] Government Accountability Office, *Sex Trafficking: Online Platforms and Federal Prosecutions* (GAO Publication No. 21-385) (June 2021) (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).

[13] *See Online Platforms and Sex Worker Discrimination*, Hacking//Hustling (last visited May 1, 2023) (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).

[14] *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) (quoting a researcher at the University of Pittsburgh describing

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.[15] 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 by making certain that only the sender and receiver can view them. It does this by ensuring that the keys used to encrypt and decrypt data are known only to the sender and the authorized recipients of the data. Billions of people worldwide rely on encryption to secure their daily activities online, from web browsing to online banking to communicating with friends and family.[16]

Everyone who communicates with others on the internet should be able to do so privately. However, this security is especially relied upon by journalists,[17] Congress,[18] the military,[19] domestic violence survivors,[20] union organizers,[21] immigrants,[22] and anyone who seeks to keep their communications secure from malicious hackers. Since the Supreme Court's decision in *Dobbs v. Jackson Women's Health Organization*, encryption has become even more important for healthcare workers and pregnant people, who are increasingly at risk of prosecution under state laws that criminalize abortion or sharing information about reproductive healthcare. Police in states where abortion is illegal have already used unencrypted digital evidence for prosecutions.[23] Experts routinely recommend that people seeking abortions use encrypted services, and some women's healthcare providers say they rely heavily on encrypted forms of communication.[24]

---

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) (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").

[15] See Danielle Blunt & Ariel Wolf, *Erased The Impact of FOSTA-SESTA*, Hacking//Hustling (2020); Makena Kelly, *Democrats want data on how sex workers were hurt by online crackdown*, The Verge (Dec. 17, 2019).

[16] *See* Internet Society & Center for Democracy & Tech., *Internet Impact Brief How the US EARN IT Act Threatens Security, Confidentiality, and Safety Online* (Nov. 16, 2022).

[17] Internet Society & Committee to Protect Journalists, *Encryption How It Can Protect Journalists and the Free Press*, ISOC (Mar. 2020).

[18] Zach Whittaker, *In encryption push, Senate staff can now use Signal for secure messaging*, ZDNet (May 16, 2017).

[19] 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).

[20] Kaitlyn Well & Thorin Klosowski, *Domestic Abusers Can Control Your Devices. Here's How to Fight Back*, N.Y. Times Wirecutter (Apr. 6, 2020).

[21] Lorenzo Franceschi-Bicchierai & Lauren Kaori Gurley, *How to Organize Your Workplace Without Getting Caught*, Vice Motherboard (Jan. 15, 2020).

[22] *Data Encryption: Why It's Vital for Migrants and their Defenders*, PICUM (Mar. 1, 2023); *Top 6 Digital Safety Tips for Undocumented Folks*, United We Dream (June 2, 2020).

[23] *See, e.g.*, Shaila Dewan & Sheera Frenkel, *A Mother, a Daughter and an Unusual Abortion Prosecution in Nebraska*, N.Y. Times (Aug. 18, 2022) (reporting that private Facebook messages between a mother and daughter "obtained by the police through a warrant, have become key evidence in a rare prosecution over abortion").

[24] Kevin Collier, *Looming abortion law changes are pushing clinics to take a look at digital privacy*, NBC News (June 8, 2022) (reporting that "[s]ome clinic employees say they are embracing encrypted messaging apps and Zoom meetings to leave less of an electronic paper trail"); Heather Kelly, Tatum Hunter & Danielle Abril, *Seeking an*

EARN IT puts Americans, U.S. businesses, and everyone around the world at great risk of harm online by strongly disincentivizing providers from providing strong encryption. It does so in two main ways.

First, EARN IT would permit states to seek to impose criminal or civil liability on intermediaries who offer encryption, by arguing that the use of encryption is evidence under state law that a service acted recklessly or negligently in failing to identify CSAM. In the face of the risk of civil and criminal liability, many services will decide not to offer encrypted services.

Although Section 5(7)(A) purports to protect the ability of intermediaries to offer encryption,[25] it actually does the opposite. Section 5(7)(A) states merely 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. (Emphasis added). At the same time, Section 5(7)(B) specifies that courts will remain able to consider information about whether and how an intermediary employs end-to-end encryption as evidence in cases brought under EARN IT. Together, these provisions explicitly *allow* courts to consider the offering of end-to-end encrypted services as evidence of an intermediary's guilt of crimes related to CSAM.[26] While prosecutors and plaintiffs could not claim that providing encryption, alone, was enough to prove 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.

This risk that encryption could be used as evidence against them in state proceedings will discourage intermediaries from offering it. Small "mom and pop" intermediaries that could be bankrupted by a single lawsuit will be especially deterred from offering encryption. For all intermediaries, the mere threat that use of encryption could be used as evidence against an intermediary in a civil suit or criminal prosecution will serve as a strong disincentive to deploying encrypted services in the first place.

Second, 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

---

abortion? Here's how to avoid leaving a digital trail, Wash. Post (Aug. 12, 2022) (recommending pregnant people seeking an abortion use encrypted messaging apps).

[25] Section 5(7)(A) states that "none of the following actions or circumstances shall serve as an independent basis for liability of a provider of an interactive computer service for a claim or charge described in [paragraph 6]:"

> (i) The provider utilizes full end-to-end encrypted messaging services, device encryption, or other encryption services.
> (ii) The provider does not possess the information necessary to decrypt a communication.
> (iii) The provider fails to take an action that would otherwise undermine the ability of the provider to offer full end-to-end encrypted messaging services, device encryption, or other encryption services.

[26] This language was originally proposed in the 116th Congress's House companion bill to EARN IT. H.R. 8454, 116th Cong. (EARN IT Act of 2020). At the time, experts criticized this language as undermining encryption. *See* Riana Pfefferkorn, *House Introduces EARN IT Act Companion Bill, Somehow Manages to Make It Even Worse* (Oct. 5, 2020).

services. Given the oft-stated opposition of federal officials to encryption,[27] the Commission could well recommend against offering end-to-end encryption and recommend providers adopt techniques that ultimately weaken their product's cybersecurity. While these "best practices" would be voluntary, they could cause reputational harm to providers if they choose not to comply. Refusal to comply could also be considered as evidence in support of a provider's liability, and inform how judges evaluate cases against providers. States may even amend their laws to mandate the adoption of these supposed best practices. The lack of clarity and fear of liability, in addition to potential public shaming, will likely disincentivize many companies from offering strong encryption, at a time when we should be encouraging the opposite.

The EARN IT Act Risks Undermining Child Abuse Prosecutions

Finally, the EARN IT Act risks undermining child abuse prosecutions by transforming providers into agents of the government for purposes of the Fourth Amendment.[28] 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.[29] 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.[30]

***

The EARN IT Act would have devastating consequences for everyone's 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, and it should commit to conducting a full, independent internet impact assessment to identify potential harms

---

[27] *See, e.g.*, Kate Fazzini, *FBI Director Wray: I strongly share Barr's concerns about encrypted devices and messaging platforms, cites Sutherland Springs Apple case*, CNBC (July 25, 2019); Tonya Riley, *The Cybersecurity 202: FBI renews attack on encryption ahead of another possible attack on the Capitol*, Wash. Post (May 4, 2021); Joseph Marks, *The Cybersecurity 202: The Justice Department is racking up wins despite encryption concerns* (June 16, 2021) (reporting that "Attorney General Merrick Garland warned during congressional testimony . . . that encryption allows terrorists to communicate online with greater secrecy than before" and that Biden and then-UK Prime Minister Boris Johnson pledged in a joint statement to "'work together to maintain tightly-controlled lawful access to communications content that is vital to the investigation and prosecution of serious crimes including terrorism and child abuse'").

[28] 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).

[29] *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").

[30] 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).

likely to result from any internet-related legislation, such as harms to users' freedom of expression and privacy, before the legislation is voted upon.

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 the Internet Society's Natalie Campbell, Senior Director, North American Government and Regulatory Affairs at campbell@isoc.org.

Sincerely,

The 6:52 Project Foundation, Inc.
Access Now
Advocacy for Principled Action in Government
Advocates for Youth
Advocating Opportunity
Africa Media and Information Technology Initiative (AFRIMITI)
AIDS United
American Atheists
American Civil Liberties Union
American Humanist Association
American Library Association
Amnesty International USA
ANSWER Detroit
Arkansas Black Gay Men's Forum
Aspiration
Assembly Four
Associação Portuguesa para a Promoção da Segurança da Informação (AP2SI)
Association for Queer Anthropology
Association of Research Libraries (ARL)
Athlete Ally
Blogger On Pole
Center for Democracy & Technology
Centre for Multilateral Affairs (CfMA), Uganda
Charity for People Powered Democracy
COLAGE
Collaboration on International ICT Policy for East & Southern Africa (CIPESA)
comun.al, Digital Resilience Lab (Mexico)
Cyberstorm.mu
Dangerous Speech Project
DEF CON 864 (DC864)
Defending Rights & Dissent
Demand Progress
Digital Empowerment Foundation
EducateUS: SIECUS In Action
EFF-Austin
Electronic Frontier Foundation (EFF)
Electronic Frontiers Georgia
Encrypt Uganda
EQTX Equality Texas
Equality Arizona
Equality California
Equality Federation
Equality New Mexico
Erotic Service Provider Legal Education and Research Project (ESPLERP)
EveryLibrary Institute
Fairness Campaign
Fight for the Future
Foundation for Individual Rights and Expression
Free Press Action
Free Speech Coalition
Freedom Network USA
Freedom Oklahoma
Future Ada
Georgia Equality
Georgia Tech Internet Governance Project
GLAAD
GoodWorks
Government Information Watch
Hawai'i Health & Harm Reduction Center
Health Not Prisons Collective
Hep Free Hawai'i
HIPS
Human Rights Campaign
In Our Own Voices, Inc.
Indivisible Bainbridge Island
Indivisible Fighting 9

Indivisible Plus Washington
Indivisible Skagit
Indivisible Washington's 8th District
International Online Safety Corp (IOSCORP)
Internet Safety Labs
Internet Society
ISOC Brazil - Brazilian Chapter of the Internet Society
JCA-NET(Japan)
LGBT Technology Partnership
Louisiana Trans Advocates
MassachusettsTransgender Political Coalition
May First Movement Technology
Mazzoni Center
MEGA Limited
Mozilla Foundation
Myntex Inc
National Center for Lesbian Rights
National Coalition Against Censorship
National Lawyers Guild
New America's Open Technology Institute
New Moon Network
North Kitsap Indivisible
Nupef
Oakland Privacy
Old Pros
OpenMedia
OPTF
Organization for Identity & Cultural Development (OICD.net)
PDX Privacy
PEN America
Peninsula Peace and Justice Center
Positive Women's Network-USA
Privacy & Access Council of Canada
PrivaZy
Progressive Technology Project
Public Knowledge
Raging Grannies Action League
Ranking Digital Rights
Reframe Health and Justice
Restore The Fourth
Sex Workers Project of the Urban Justice Center
Snohomish County Indivisible
Society for Visual Anthropology
State Innovation Exchange Action (SiX Action)
(S.T.O.P.) - The Surveillance Technology Oversight Project
Students United for Palestinian Rights, Michigan State University
SWOP Behind Bars Inc
SWOP-USA
Tech for Good Asia
TechFreedom
The Copia Institute
The Tor Project
Transgender Education Network of Texas (TENT)
Transgender Law Center
TransOhio
Tutanota
TwelveDot Incorporated
UM-Dearborn Muslim Students Association
Unitarian Universalist Association
University of Bosaso
University of Michigan-Dearborn Pride Student Organization
WA People's Privacy
Whidbey Indivisible
Wikimedia Foundation
Woodhull Freedom Foundation
X-Lab
Yale Privacy Lab