March 3, 2022

The Honorable Richard Durbin
Chairman, Senate Committee on the Judiciary
711 Hart Senate Office Building
Washington, DC 20510

The Honorable Chuck Grassley
Ranking Member, Chair, Senate Judiciary Committee
United States Senate
135 Hart Senate Building
Washington, DC 20510

cc: Members of the Senate Committee on the Judiciary

Re: S.3538, The EARN IT Act

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

We, the undersigned, write to express our concerns about the threats to liberty, security, and the safety of children posed by S.3538, the Eliminating Abusive and Rampant Neglect of Interactive Technologies Act of 2022 (EARN IT Act). As introduced, the 2022 EARN IT Act adopts many of the worst aspects of its 2020 predecessor, and magnifies their harmful effects.

Far from protecting children, the EARN IT Act's current language will instead imperil criminal prosecution of the vilest crimes against children, leaving them even more vulnerable to predators who walk free. By wielding expansive and uncertain liability as a cudgel to compel private companies to monitor users' communications, this bill risks converting those otherwise voluntary efforts into state action requiring a warrant under the Fourth Amendment — potentially leading to reversed convictions and withdrawn or stymied prosecutions. Thus, the bill will do the opposite of what its sponsors claim. Compelling monitoring means coercing companies not to secure their services with end-to-end encryption, because E2EE makes monitoring difficult, if not impossible. It may also mean coercing companies into installing backdoors into their services or devices. Both undermine the privacy, security and safety of law-abiding users. Secure encryption is vital to protect private communications from thieves, repressive or hostile foreign governments, wayward government agencies, and other malicious actors.

The Supreme Court has extended the Fourth Amendment's strictures to ostensibly private actors when "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.'" *U.S. v. Stevenson*, 727 F.3d 826, 829 (8th Cir. 2013) (quoting *Skinner v. Railway Labor Executives' Assn*, 489 U.S. 602, 615 (1989)). Today, tech companies cooperate voluntarily with law enforcement to identify those who create, traffic in, and consume child sexual abuse material (CSAM), but courts have held that they are not state actors subject to the Fourth Amendment. The EARN IT Act would give CSAM defendants compelling

arguments that the evidence used to prosecute them was obtained by companies conducting warrantless searches under legal pressure, transforming them into state actors.

EARN IT effects such pressure primarily by exposing companies to unprecedented liability under state criminal and civil laws. Each state could define each of the grounds for liability in whatever way it chooses, and worse, with whatever *mens rea* or scienter standard it chooses. Companies may find themselves liable in some jurisdictions not because they had "actual knowledge" of CSAM, but under the much lower standards of "recklessness" or "negligence." The specter of liability under such standards will inevitably force companies to take preventative measures to monitor for CSAM, which requires not using strong encryption.

At this Committee's markup of this bill in July 2020, Sen. Lee proposed to avoid both the constitutional problem and the privacy and security problem. His amendment attempted to harmonize state-level liability with federal law by requiring that any conduct underlying a state criminal prosecution or state civil claims constitute a violation of 18 U.S.C. §§ 2252 or 2252A. Sen. Lee withdrew his amendment on the understanding that the bill's sponsors would work with him to address his concerns on the Senate floor before any final vote. No such changes were made when EARN IT was reintroduced.

Maintaining a consistent body of criminal law for the Internet was one of the original goals of Section 230. If that law proves inadequate, it should be updated, as it was when Congress enacted FOSTA in 2017,[1] but still remain uniform. The Lee amendment would greatly reduce the problem of having a patchwork of 56 state and territorial criminal laws, enforced according to the whims of local prosecutors and courts.

Likewise, harmonizing state civil claims with Sections 2252 and 2252A would avoid a patchwork in which one state law can compromise the security of Internet services nationwide. Rather than permitting states to impose liability for any claims they might invent, the Lee amendment would limit the scope of potential civil liability to violations of federal law, including the actual knowledge requirement. Meritorious claims could proceed but without imposing unmanageable potential liability limited only by the political motivations of state attorneys general and the creativity of plaintiffs' lawyers.

But even the standard supplied by federal law in civil cases is problematic as applied to tech companies rather than the individuals who might abuse their services to share CSAM. EARN IT would still allow tech companies to be sued based on claims that they had "knowledge" of the CSAM. Knowledge standards are unworkable for civil liability in this context because even unsubstantiated complaints about unlawful material may, in some circumstances, suffice to establish "knowledge." Tying civil liability to knowledge recreates the very "Moderator's Dilemma" that led Congress to enact Section 230 in the first place: it creates a perverse incentive for websites to avoid gaining knowledge that could lead to liability, such as through monitoring or moderating communications.[2]

---

[1] H.R.1865, 115th Cong. (2018).

[2] Even with the Lee amendment, EARN IT would still, for the first time, allow tech companies to be sued for content they did not create.

The 2022 EARN IT Act, as introduced, claims to protect encryption while simultaneously attacking it. This presents a serious threat to technology that enables commerce, safeguards the data of everyday law-abiding citizens, and protects activists around the world as they organize to fight against repressive authoritarian regimes — to name only a few benefits.

In 2020, Sen. Leahy introduced an amendment, accepted at markup, to the previous version of EARN IT to mitigate this concern and protect companies from facing liability for their decision to offer E2EE services or failing to create security flaws in their products to enable monitoring. While the current version of EARN IT Act includes the same list of protected activities as the Leahy amendment, it actively undermines the very purpose of that amendment by affirmatively permitting courts to consider the use of encryption, inability to decrypt messages, or refusal to build backdoors as evidence to support other claims. As discussed above, state criminal or civil laws may have lower *mens rea* or scienter standards, and this provision all but ensures that the use of (or failure to compromise) encryption will be used as evidence to prove that mental state. This is tantamount to holding companies directly liable for encryption.

But even reverting to the original Leahy amendment would not completely mitigate concerns about the Fourth Amendment concerns, privacy or security. While it protected companies from liability for being unable to conduct searches, the amendment did not protect them from refusing to conduct such searches—the more direct Fourth Amendment and privacy problem. A company offering E2EE products might still be coerced into compromising the security of its devices by scanning user communications "client-side" (*i.e.*, on the device) prior to encrypting sent communications or after decrypting received communications.[3] This not only raises Fourth Amendment concerns, but also harms the privacy and security of users. The capacity to conduct such surveillance presents an inherent risk of being exploited by malicious actors. Some companies may be able to successfully safeguard such surveillance architecture from misuse or exploitation. But resources and approaches will vary across companies, and it is a virtual certainty that not all of them will be successful. Accordingly, it is vital that the Leahy amendment not only be restored, but reinforced to protect against mandates — explicit or implicit — that companies affirmatively monitor their users' communications.

Thank you for your attention to our concerns. We would be happy to assist your Committee in working to revise the EARN IT Act to ensure that the bill advances rather than subverts its goal of protecting children, and does not undermine the strong security fundamental to online communications and commerce. Please contact Ari Cohn <acohn@techfreedom.org> with any questions you may have.

See Letter from TechFreedom to Senate Judiciary Committee at 6-12 (Feb. 8, 2022) https://techfreedom.org/wp-content/uploads/2022/02/TechFreedom-Letter-re-EARN-IT-Amendments-for-Markup-2.8.22.pdf.

[3] "Theoretically, a system that uses client-side scanning could still send messages encrypted end to end, and so the Leahy amendment would not offer any protection…" Hannah Quay-de la Vallee & Mana Azarmi, *The New EARN IT Act Still Threatens Encryption and Child Exploitation Prosecutions*, CDT (Aug. 25, 2020), https://cdt.org/insights/the-new-earn-it-act-still-threatens-encryption-and-child-exploitation-prosecutions/.

Sincerely,

Organizations

Americans for Prosperity

Competitive Enterprise Institute

National Taxpayers Union

R Street Institute

Taxpayers Protection Alliance

TechFreedom

Individuals (affiliations listed for identification purposes only)

Jeffrey Westling, American Action Forum