TECHFREEDOM
LAW FOR A DYNAMIC FUTURE

771.200.4997
Washington, DC
techfreedom.org

May 2, 2023

The Honorable Richard J. Durbin
Chair, Senate Judiciary Committee
United States Senate
711 Hart Senate Building
Washington, DC 20510

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

Re: EARN IT Act of 2023 (S. 1207)

Dear Chair Durbin, Ranking Member Graham, and Members of the Committee:

We write to reiterate our grave concerns about the EARN IT Act, as reintroduced in the 118th Congress. By coercing companies into abandoning strong, end-to-end encryption, EARN IT places the private communications of all users at the mercy of thieves, repressive or hostile foreign governments, and wayward government agencies here at home. Moreover, rather than advancing the fight against child sexual exploitation (CSE) and child sexual abuse material (CSAM), EARN IT will *undermine* prosecutions for these vile crimes.

As introduced, EARN IT dramatically increases the risk of liability for any service that offers end-to-end encryption. Under EARN IT, the use of encryption (or the failure to weaken that encryption) cannot serve as an *independent* basis for liability.[1] But EARN IT expressly *permits* courts to consider the use of encryption as evidence to support other claims[2]—including under state laws with a lower *mens rea* requirement.[3] While federal CSE and CSAM statutes require "actual knowledge,"[4] state laws may permit liability based on "recklessness" or "negligence."[5] If a company's use of strong encryption that leaves it unable to detect and

---

[1] EARN IT Act of 2023, S. 1207, 118th Cong. § 5(7)(A).

[2] EARN IT Act of 2023, S. 1207, 118th Cong. § 5(7)(B).

[3] *See* EARN IT Act of 2023, S. 1207, 118th Cong. § 5(6)(B) (permitting prosecutions under state laws regarding the "advertisement, promotion, presentation, distribution, or solicitation" of CSAM without requiring that the offenses constitute a violation of federal law.).

[4] *See, e.g.*, 18 U.S.C. §§ 2251(d), 2252(a).

[5] Some existing state laws already impose these lower *mens rea* requirements. *See, e.g.*, ARK. CODE § 5-27-604 (2010); MD. CODE § 11-208 (2020); FLA. STAT. § 847.0137 (2021); GA. CODE § 16-12-100.1 (2010). *See also* Ben Horton, *EARN IT's State-law Exemption Would Create Bewildering Set of Conflicting Standards for Online Speech*, CDT (Aug. 11, 2020), https://cdt.org/insights/earn-its-state-law-exemption-would-create-bewildering-set-of-conflicting-standards-for-online-speech/.

block such messages can be considered as evidence of negligence or recklessness, the net result would be nearly the same as permitting liability for encryption itself. Few, if any, companies will risk offering encrypted services in the face of this potential liability.

This result is especially troubling in light of recent concerns about who has access to Americans' private communications and data. When Elon Musk alleged that the federal government previously had "full access" to users' private direct messages on Twitter, members of Congress expressed concern. Senator Ted Cruz asked: "Is Facebook allowing the feds to monitor Messenger & WhatsApp?"[6] In fact, end-to-end encryption allays one of Senator Cruz's concerns: because WhatsApp is end-to-end encrypted, only the sender and recipient can view the messages.[7] To provide similar assurances, Musk announced that Twitter would encrypt direct messages "with the hopes of limiting government interference."[8] While the veracity of Musk's allegation has been disputed,[9] his premise is correct: lack of encryption makes such intrusions possible.

Lawmakers have also expressed concerns about how foreign adversaries, such as the Chinese Communist Party, might obtain private information about U.S. citizens. While most of the concern has focused on TikTok, a recent report indicates that a state-sponsored Chinese hacking group is actively targeting companies—including social media and telecommunications companies—to collect intelligence.[10] Coercing companies into abandoning end-to-end encryption places our private communications at risk; it means information obtained by malicious actors will be unencrypted and thus usable.

Finally, EARN IT will undermine, not assist, prosecutions for CSE and CSAM offenses. EARN IT clearly aims to force companies to do more to combat CSAM, including by monitoring user communications and searching for offending content (facilitated by the abandonment of

---

[6] @tedcruz, TWITTER (Apr. 17, 2023, 10:58 PM), https://twitter.com/tedcruz/status/1648158910409490432. *See also* @Jim_Jordan, TWITTER (APR 18, 2023, 1:11 PM), https://twitter.com/Jim_Jordan/status/1648373801950887942 ("According to @ElonMusk, U.S. intel agencies had access to private Twitter messages . . . Just what everyone wanted!").

[7] *About end-to-end encryption*, WHATSAPP, https://faq.whatsapp.com/820124435853543 (last visited May 2, 2023).

[8] Yael Halon, *Elon Musk reveals US intel agencies had 'full access' to private Twitter DMs, discloses new encryption feature*, FOX NEWS (Apr. 17, 2023, 9:58 PM), https://www.foxnews.com/media/elon-musk-us-intel-agencies-full-access-private-twitter-dms-discloses-new-encryption-feature.

[9] Mike Masnick, *Elon Musk Is Full Of Shit, Again. No, Federal Agencies Did Not Have 'Full Access' To DMs*, TECHDIRT (Apr. 18, 2023, 9:33 AM), https://www.techdirt.com/2023/04/18/elon-musk-is-full-of-shit-again-no-federal-agencies-did-not-have-full-access-to-dms/.

[10] David Rising, *Report: Chinese state-sponsored hacking group highly active*, AP News (Mar. 30, 2023), https://apnews.com/article/china-hacking-report-redgolf-insikt-88a76977ce50d6d28d7a1be5130a1aa7.

strong encryption).[11] But coercing companies into conducting such monitoring or searches under the threat of broad liability would likely transform their efforts into state action subject to the Fourth Amendment.[12] Because private companies cannot obtain a warrant, evidence obtained from such activities would be inadmissible in court—allowing predators to go free. To avoid precisely this outcome, Congress made clear that, while service providers are required to report CSAM and CSE to the National Center for Missing and Exploited Children,[13] they are *not* required by law to engage in monitoring, searching, or screening of communications.[14] In contrast, EARN IT would coerce companies into retaining access to private communications and allow liability under broad state laws to coerce monitoring, searching, and screening. By triggering the Fourth Amendment's warrant requirement, such coercion would frustrate prosecution of these heinous crimes against children—an outcome nobody desires.

—

We explained these—and other—concerns in more detail, and proposed amendments that may ameliorate them to some degree, in our letter prior to last year's markup of EARN IT. We have enclosed that letter for your reference.[15] Thank you for your attention to these important matters. We would be happy to assist your committee in working to revise the EARN IT Act to ensure that it facilitates, rather than frustrating, the enforcement of CSE and CSAM laws, and that it does not harm the privacy, security, and safety of law-abiding users.

Sincerely,

Ari Cohn
Free Speech Counsel, TechFreedom
acohn@techfreedom.org

Berin Szóka
President, TechFreedom
bszoka@techfreedom.org

Encl.

---

[11] At markup last year, Senator Lindsey Graham stated "Our goal is to tell the social media companies 'get involved and stop this crap. And if you don't take responsibility for what's on your platform, then Section 230 will not be there for you." Senator Chris Coons added that he was "hopeful that this will send a strong signal that technology companies . . . need to do more."

[12] *See* 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)) ("Even when a search is not required by law . . . 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] 18 U.S.C. § 2258A(a)(2).

[14] 18 U.S.C. § 2258A(f).

[15] That letter can also be accessed at: https://techfreedom.org/wp-content/uploads/2022/02/TechFreedom-Letter-re-EARN-IT-Amendments-for-Markup-2.8.22.pdf