

TechFreedom  
110 Maryland Ave, NE Suite 205  
Washington, DC 20002



June 30, 2020

The Honorable Lindsey Graham  
Chairman, Senate Judiciary Committee  
United States Senate  
Russell Senate Office Building 290  
Washington, D.C. 20510

The Honorable Diane Feinstein  
Ranking Member, Senate Judiciary Committee  
United States Senate  
Hart Senate Office Building 331  
Washington D.C. 2051

cc: members of the Senate Judiciary Committee

**re: Senate Judiciary Committee Markup of the EARN IT Act of 2020 (S.3398)**

Dear Chairman Graham and Ranking Member Feinstein:

We write to express our concerns about the EARN IT Act, a well-intentioned but fundamentally flawed piece of legislation.

The EARN IT Act will hurt, not help, children. The bill risks making it impossible for tech companies to continue cooperating with law enforcement to stop the spread of child sexual exploitation (CSE) content and child sexual abuse material (CSAM). Currently, tech companies do not obtain a warrant from a judge before searching their services for evidence of CSE/CSAM violations, or turning over such evidence to the government via the National Center for Missing and Exploited Children (NCMEC). In *Ackerman*, now-Justice Gorsuch ruled that NCMEC was a government agent subject to the Fourth Amendment's warrant requirement.<sup>1</sup> The EARN IT Act could lead a court to reach the same conclusion about tech companies themselves. If so, the EARN IT Act would *prevent* them from doing the very thing it aims to force them to do: collect evidence of child abuse. Such a decision would also jeopardize the criminal convictions of anyone prosecuted based on such evidence.

The only way to avoid this Fourth Amendment problem would be to drop the bill's amendments to 18 U.S.C. § 2255 and 47 U.S.C. § 230 (so the bill would merely create an advisory commission). Together, these amendments create sweeping new civil liability for interactive computer service (ICS) providers for failing to prevent all transmission of CSE/CSAM by users: instead of being liable for "actual knowledge" of such material, ICS

---

<sup>1</sup> *United States v. Ackerman*, 831 F.3d 1292 (10th Cir. 2016).

providers could be held “reckless” for not designing their services to prevent any truly private communications, prevent adults from communicating with children, *etc.* There is no way to limit these effects to CSE/CSAM: The only way to prevent bad uses of Internet services is to fundamentally re-engineer them for *all* users for *all* content.

***End-to-End Encryption.*** Online communications services would face massive civil liability for offering “end-to-end” encryption, in which only the users hold the encryption keys and the service provider cannot access the communications in unencrypted form. The Department of Justice clearly believes offering such “strong” encryption is inherently reckless, but the alternative (requiring service providers to retain the ability to view the contents of private communications) means building inherently insecure systems. There is no such thing as a backdoor only for the good guys: requiring a backdoor access for U.S. law enforcement and national security agencies exposes users’ private communications to attack by foreign governments and malicious hackers.

***Other Mandates.*** The EARN IT Act could require other design changes, including filtering all traffic, retaining more data about users, and age-verifying all users in order to prevent minors from using some services and to prevent adults from communicating with minors. Requiring users to prove their age (usually by providing a credit card number) means requiring them to identify themselves, which intrudes on their right to anonymous speech. In effect, the EARN IT Act would essentially revive the Child Online Protection Act of 1998—and would be unconstitutional for the same reasons the courts struck down COPA.

***Constitutional Concerns.*** The EARN IT Act’s convoluted structure will not prevent courts from recognizing the bill for what it is: thinly veiled coercion of private companies to violate the constitution. In addition to violating the Fourth Amendment, the bill violates the First Amendment by forcing ICS providers to redesign their services in ways that burden the rights of adult users to access lawful content anonymously. This also intrudes on the First Amendment right of Internet services to design their services as they see fit and compels them to rewrite their code, a recognized form of speech.<sup>2</sup> It makes no difference that the EARN IT Act works its coercion indirectly—by making ICS providers fear liability for their design decisions, then allowing them to “earn” back their Section 230 liability shield by complying with *all* of a set of nominally voluntary “Best Practices” developed by an expert Commission under the direction of the Attorney General. The Supreme Court has clearly rejected such unconstitutional conditions.<sup>3</sup>

The bill purports to offer an alternative liability shield: allowing ICS providers to show the “reasonableness” of their practices. This affirmative defense will be so difficult to prove that it will be of limited value: websites sued for “recklessly” facilitating CSE/CSAM transmission

---

<sup>2</sup> *Bernstein v. United States Dept. of Justice*, 176 F.3d 1132, 1146 (9th Cir. 1999).

<sup>3</sup> *See, e.g., Agency for Int’l Dev. v. All. for Open Soc’y Int’l, Inc.*, 570 U.S. 205 (2013).

would have to incur great expense litigating such suits through discovery and a motion for summary judgment, if not trial.

The only effective way to regain Section 230's shield against litigation would be to certify compliance with all of the "Best Practices." This makes them *de facto* mandates. Circumscribing their scope may help to limit their effectively regulatory effects, but this would not solve the bill's underlying problems: the "recklessness" standard for liability and "reasonableness" affirmative defense are unconstitutionally vague and will burden constitutionally protected speech, not just CSE/CSAM. Regardless of what the "Best Practices" say, or whether they are ever finalized, ICS providers will be forced to design less secure services that curtail their users' First Amendment rights.

Finally, the bill unconstitutionally cedes lawmaking powers to a private body. Having the House and Senate rubber-stamp the Commission's "Best Practices" does not remedy this problem.<sup>4</sup> Indeed, making what amounts to a new law (*de facto* conditions on Section 230 eligibility) without the signature of the President (or an opportunity to veto the bill) violates the Constitution's Presentment Clause.<sup>5</sup>

In short, there is no way to remedy the constitutional problems created by the EARN IT Act. We urge you to discard this unworkable piece of legislation and start over. The focus should be on maximizing the enforcement of existing child protection criminal law — which Section 230 has never limited. Congress must remedy chronic underfunding for the enforcement of existing federal CSE/CSAM laws. Nor do we need a new law to enlist state, local and tribal prosecutors in the fight against CSAM; the Attorney General already has the authority to empower them to enforce federal law, but has chosen not to do so. Lawmakers must directly confront the difficult questions of what more the Fourth and First Amendments will permit the government to do to stop the spread of CSE/CSAM — questions that are addressed in the attached white paper.<sup>6</sup> The following one-page summary distills our concerns about the bill.

Sincerely,

TechFreedom

---

<sup>4</sup> *Carter v. Carter Coal Co.*, 298 U.S. 238, 311 (1936); *Gundy v. United States*, 139 S. Ct. 2116, 2121 (2019).

<sup>5</sup> *Immigration and Naturalization Service v. Chadha*, 462 U.S. 919, 958 (1983).

<sup>6</sup> Berin Szóka, *The Unconstitutional, Unworkable EARN IT Act*, Media Law Resource Center Bulletin, "Legal Frontiers in Digital Media" (June 2020), available at <https://bit.ly/38gNq8n>.

# The Truth About the EARN IT Act: It will HURT, not help, children

- Attempts at clever legislative drafting can't hide fundamental constitutional missteps. Merely "outsourcing" constitutional violations to a private body doesn't solve the problem.
- Congress can't require the surrendering of core constitutional rights in exchange for a benefit (Section 230 immunity). *Agency for Int'l Dev. v. All. for Open Soc'y Int'l, Inc.*, 570 U.S. 205 (2013).

## 1st Amendment Problems

- The "Recklessness" standard is **overbroad**: it will force changes in the design of Internet services that necessarily burden fully protected, lawful speech.
- Limiting the ability of **users** to access constitutionally protected materials, just like the CDA (1996), struck down in *Reno v. ACLU*, 521 U.S. 844, 867-68 (1997), and COPA (1998), struck down in *ACLU v. Mukasey*, 534 F.3d 181 (3d Cir. 2008).
- Websites enjoy full First Amendment rights; any attempts to regulate speech subject to **strict scrutiny**. *Brown v. Entertainment Merchants Ass'n*, 132 S.Ct. 81 (2011).
- Coerces platforms into changing their **editorial practices** in order to "earn" back Section 230 immunity, vital to hosting third-party content which drives the Internet ecosystem. *Miami Herald Publ'g Co. v. Tornillo*, 418 U.S. 241, 258 (1974).
- Acts as a **prior restraint**, *Nebraska Press Ass'n v. Stuart*, 427 U.S. 539, 559 (1976), on encryption, which courts have recognized as a form of speech, *Bernstein v. DOJ*, 176 F.3d 1132, 1146 (9th Cir. 1999).
- **Compels speech** in violation of the First Amendment. *Riley v. Nat'l Fed'n of the Blind of N.C., Inc.*, 487 U.S. 781, 798 (1988).

## 4th Amendment Problems

- **Voluntary** system of warrantless reporting of CSE/CSAM converted to coercive system, turning carriers into **state actors** (as NCMEC is), thus requiring **warrants** for carriers to search for and turn over CSE/CSAM. *United States v. Ackerman*, 831 F.3d 1292 (10th Cir. 2016).
- **Sexual predator convictions** based on "tainted" evidence could be tossed out.
- The EARN IT Act would have exactly the **opposite** effect of what its drafters claim they want: making enforcement **harder**.

## Other Constitutional Problems

- **Fifth Amendment**. "Recklessness Standard" is **void for vagueness**. *Coates v. City of Cincinnati*, 402 U.S. 611, 616 (1971) (Black, J. concurring).
- Handing off regulatory powers to an independent commission violates the **Nondelegation Doctrine**. *Carter v. Carter Coal Co.*, 298 U.S. 238, 311 (1936); *see Gundy v. United States*, 139 S. Ct. 2116, 2121 (2019).
- Congressional approval process (without presidential sign-off) violates the **Presentment Clause**. *Immigration and Naturalization Service v. Chadha*, 462 U.S. 919, 958 (1983).

**Conclusion:** The EARN IT Act has virtually **nothing** to do with child safety, and everything to do with trying to:

- Control the editorial judgments of large tech companies;
- Discourage adoption of secure end-to-end encryption.

June 30, 2020

For a deeper analysis, visit <https://bit.ly/38gNq8n>

**TECH  
FREEDOM**