epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

March 11, 2020

The Honorable Chuck Grassley, Chairman
The Honorable Diane Feinstein, Ranking Member
Committee on the Judiciary
U.S. Senate Committee on the Judiciary
Dirksen Senate Office Building 224
Washington, DC 20510

Dear Chairman Graham and Ranking Member Feinstein:

We write to you regarding the hearing on "The EARN IT Act: Holding the Tech Industry Accountable in the Fight Against Online Child Sexual Exploitation."[1] EPIC recognizes the legitimate concerns about the distribution of child sexual exploitation material ("CSAM") and support efforts to reform Section 230 of the Communications Decency Act.[2] Regarding the development of Best Practices that the Act would establish, we caution against recommendations that would reduce privacy and security for Internet users.

The Electronic Privacy Information Center ("EPIC") is a public interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues and to protect privacy, freedom of expression, and democratic values in the information age.[3] EPIC has advocated for strong encryption since its founding.[4] EPIC also played a key role in the development of the international framework for cryptography policy that favored the deployment of strong security measures to safeguard personal information and promote online commerce. EPIC published the first comparative studies of international encryption policy.[5]

EPIC also supports efforts to reform Section 230. In the case *Herrick v, Grindr*,[6] EPIC provided an amicus brief for the Second circuit in which we explained that the "Internet has changed since Congress passed the [Communication Decency Act] in 1996. Advanced social media platform did not exist when Congress enacted the law."[7] We objected to a lower court interpretation of section 230, which found that "online platforms bear no responsibility for the harassment and abuse their

[1] *The EARN IT Act: Holding the Tech Industry Accountable in the Fight Against Online Child Sexual Exploitation: Hearing Before the S. Comm. on the Judiciary*, 116th Cong. (Mar. 11, 2020), https://www.judiciary.senate.gov/meetings/the-earn-it-act-holding-the-tech-industry-accountable-in-the-fight-against-online-child-sexual-exploitation.
[2] 47 U.S.C. § 230.
[3] *See About EPIC*, EPIC.org, https://epic.org/epic/about.html.
[4] See e.g., EPIC, *The Clipper Chip*, https://epic.org/crypto/clipper/.
[5] EPIC, *Cryptography and Liberty 1998: An International Survey of Encryption Policy* (1998).
[6] EPIC, *Herrick v. Grindr* (2020), https://epic.org/amicus/230/grindr/.
[7] Brief of *Amicus Curiae* EPIC in Support of Appellant and Urging Reversal at 5, *Herrick v. Grindr*, 765 Fed. App'x 586 (2d Cir. 2019) (No. 18-369), *available at* https://epic.org/amicus/230/grindr/EPIC-Amicus-Herrick-Grindr.pdf.

systems enable. If they chose not to respond to the exposure of personal information or intimate images, to threats of violence, to verbal and psychological abuse, there is nothing a victim can do to intervene."[8] As we explained, "Congress never intended § 230 to create such a system."[9]

But EPIC has also recognized Fourth Amendment concerns in CSAM investigative techniques that rely on image-matching algorithms. In *US v. Miller,* we explained to the Sixth Circuit that "the private files of Gmail users are routinely subject to inspection and analysis, yet neither Google nor the federal agency has revealed the specific nature of the underlying algorithm."[10] EPIC warned that "[n]either Google nor the Government has established the accuracy, reliability, and validity of this technique. Such transparency is necessary because the consequences of an error are severe— automatic referral of a user's data, files, and identity to the National Center for Missing and Exploited Children ("NCMEC") and a subsequent investigation and referral to local law enforcement."

The Need to Adopt Section 230 Reforms To Encourage Reasonable Content Moderation

Nothing in the text, findings, or history of Section 230 indicates that Congress intended to prevent courts from protecting users who suffer abuse and harassment online. Congress made clear that it is the "policy of the United States" to "encourage the development of technologies which *maximize user control* over what information is received by individuals, families, and schools who use the Internet and other interactive computer services,"[11] and to "ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and *harassment* by means of computer."[12]

As Professor Danielle Citron has explained, "Section 230 has helped secure opportunities to work, speak, and engage online. But it has not been a clear win for civil rights and civil liberties. Its overbroad interpretation in the courts has undermined the statute's purpose and exacted significant costs to free speech and equal opportunity."[13] In recent years, platforms have been shielded from liability even where they solicit illegal activities, deliberately leave up unambiguously illegal content that causes harm, and sell dangerous products. The costs to free expression and equality have been considerable, especially for women, nonwhites, and LGBTQ individuals."[14] Professor Citron has recommended revisions to Section 230 that would "condition the legal shield on reasonable content moderation practices in the face of clear illegality that causes demonstrable harm."[15]

---

[8] *Id*. at 8.
[9] *Id*.
[10] *See, e.g.*, EPIC, *United States v. Miller* (2020) ("Whether the Fourth Amendment permits constant scanning of images uploaded to Google with corresponding reports automatically sent to law enforcement, absent evidence establishing that the underlying algorithm is accurate and reliably detects only contraband images"), https://epic.org/amicus/algorithmic-transparency/miller/.
[11] 47 U.S.C. § 230(b)(3) (emphasis added).
[12] 47 U.S.C. § 230(b)(5) (emphasis added).
[13] *Fostering a Healthier Internet to Protect Consumers: Hearing Before the H. Comm. on Energy & Commerce*, 116th Cong. 3 (2019) (statement of Danielle Keats Citron, Prof. of Law, Boston University School of Law), https://docs.house.gov/meetings/IF/IF16/20191016/110075/HHRG-116-IF16-Wstate-CitronD-20191016.pdf.
[14] *Id*.
[15] *Id.*

The Need to Protect End-to-end Encryption

We note that too few companies today actually offer "end-to-end" encryption, i.e. encrypted from the sender to the recipient. The company offering the most widely used email service in the world, for example, routinely examines private emails to identify key words in for advertising purposes. That company, and others that choose to examine message content to extract commercial value, obviously have the ability to locate CSAM, consistent with Fourth Amendment requirements.[16]

But for companies that actually provide end-to-end encryption we would caution against recommendations that diminish user privacy and security. Strong encryption is critical for network security.[17] The Act correctly identifies "data security and privacy" as relevant considerations in developing best practices.[18] The Act also requires that the Commission include two experts who have "current experience in matters related to constitutional law, consumer protection, or privacy" as well as two experts in "computer science or software engineering related to matters of cryptography, data security, or artificial intelligence in a non-governmental capacity."[19] The Act should make end-to-end encryption a "Relevant Consideration" under Section 4(a)(4).

Providing end-to-end encryption protects users, promotes commerce, and ensures cybersecurity. EPIC recommends that the EARN IT Act make clear that liability should not be imposed for a secure end-to-end encrypted communications system that safeguards the security and privacy of users.

We ask that this statement be entered in the hearing record.

EPIC looks forward to working with the Committee on these issues of vital importance to the American public.

Sincerely,

/s/ *Marc Rotenberg*
Marc Rotenberg
EPIC President

/s/ *Alan Butler*
Alan Butler
EPIC General Counsel

/s/ *Caitriona Fitzgerald*
Caitriona Fitzgerald
EPIC Policy Director

/s/ *Megan Iorio*
Megan Iorio
EPIC Appellate Counsel

[16] *See* footnote 8, supra.
[17] *See* EPIC, *Senate Considers Modest Updates to ECPA* (Sept. 16, 2015), https://epic.org/2015/09/senate-considers-modest-update.html.
[18] EARN IT Act, Sec. 4(a)(4)(B).
[19] EARN IT Act, Sec. 4(a)(2).