May 3, 2023

RE: Vote "No" On the EARN IT Act, STOP CSAM Act, and the Cooper Davis Act

Sen. Dick Durbin
Chair, Senate Judiciary Committee
711 Hart Senate Office Building
Washington, D.C. 20510

Sen. Lindsey Graham
Ranking Member, Senate Judiciary Committee
211 Russell Senate Office Building
Washington, D.C. 20510

ACLU
AMERICAN CIVIL LIBERTIES UNION

National Political Advocacy Department
915 15th Street, NW, 6th Floor
Washington, DC 20005-2112
aclu.org

Deirdre Schifeling
National Political Director

Anthony D. Romero
Executive Director

Deborah N. Archer
President

Dear Chair Durbin, Ranking Member Graham, and other members of the Senate Judiciary Committee:

The American Civil Liberties Union (ACLU) urges you to vote "No" on the EARN IT Act, the STOP CSAM Act, and the Cooper Davis Act because they would undermine free speech, privacy, and security. Collectively, these bills harm civil liberties in three ways. First, they incentivize platforms to monitor and censor their users' speech and interfere with content moderation decisions. Second, they disincentivize platforms from providing end-to-end encrypted communications services, exposing the public to abusive commercial and government surveillance practices and as a result, dissuading people from communicating with each other electronically about everything from health care decisions to business transactions. And third, they expand warrantless government access to private data. As longtime champions of privacy, free speech, and an open internet, we strongly urge you to vote against reporting these bills out of committee.

These Bills Incentivize Censorship

These bills would encourage platforms to monitor users' speech and to censor otherwise legal content by expanding the kinds of activities

that create liability[1] (for example, adding "hosting" or "facilitating")[2] and by lowering the level of awareness that a platform must have to be held liable – from actual knowledge to recklessness or negligence.[3] These changes not only expand actual liability, but also increase risk from expensive lawsuits that may ultimately be meritless, but nevertheless have to be defended.

Imposing liability when platforms do not have actual knowledge raises serious constitutional concerns under the First Amendment, which holds that distributors of content (like a bookstore or platform), cannot be held responsible for the content of the material they distribute (like books or user posts) without knowledge of that content.[4] Courts have determined that such liability would raise free speech concerns, because if bookstores or platforms were responsible for the material they distribute without awareness of its content, the public would only have access to materials that distributors can review in advance and are confident will not invite lawsuits.[5]

ACLU
AMERICAN CIVIL LIBERTIES UNION

National Political Advocacy Department
915 15th Street, NW, 6th Floor
Washington, DC 20005-2112
aclu.org

Deirdre Schifeling
National Political Director

Anthony D. Romero
Executive Director

Deborah N. Archer
President

[1] EARN IT Act, S. 1207, 118th Cong., sec. 5, § 230(e)(6)(C).
[2] STOP CSAM Act, S. 1199, 118th Cong., sec. 5(a)(6), § 2260B; *id.* sec. 6(1), § 2255(d).
[3] EARN IT Act, S. 1207, 118th Cong., sec. 5, § 230(e)(6)(C); STOP CSAM Act, S. 1199, 118th Cong., sec. 6(2), § 2255(d). Although EARN IT is silent on the mental state required for civil suits under state law, one of the bill's sponsors expressly noted the bill was intended to permit mental states other than knowledge. Statement of Sen. Blumenthal, Video: Executive Business Meeting at 2:15:39 (Feb. 10, 2022), *available at* https://www.judiciary.senate.gov/committee-activity/hearings/02/03/2022/executive-business-meeting-1 ("One [state] uses a recklessness standard [and it] happens to be that state is Illinois. Other states may wish to follow Illinois. And as Justice Brandeis said, states are the laboratories of democracy. One of the most often quoted – I think – Supreme Court comments in history, and as a former state attorney general, I welcome states using that flexibility.").
[4] Video Software Dealers Ass'n v. Webster, 968 F.2d 684, 690 (8th Cir. 1992) ("[W]e believe any statute that chills the exercise of First Amendment rights must contain a knowledge element."); accord Am.-Arab Anti-Discrimination Comm. v. City of Dearborn, 418 F.3d 600, 611 (6th Cir. 2005) (quoting *Webster*, 968 F.2d at 690); Ripplinger v. Collins, 868 F.2d 1043, 1056 (9th Cir. 1989) (partially invalidating statute that imposed liability without knowledge of the entire work); 511 Detroit St., Inc. v. Kelley, 807 F.2d 1293, 1297 (6th Cir. 1986) (requiring knowledge of the "character" of "the entire item"); Huffman v. United States, 470 F.2d 386, 402 (D.C. Cir. 1971), *on reh'g*, 502 F.2d 419 (D.C. Cir. 1974) ("Criminal liability for the sale of obscene materials requires a showing of the seller's knowledge of the content of those materials"); Davis v. State, 658 S.W.2d 572, 578 (Tex. Crim. App. 1983) ("Legislation which sanctions conviction of a bookseller, or his employee, without any proof whatsoever that he knew or was familiar with the nature of the material that was exhibited is afflicted with precisely the same vice and produces the same objectionable results as the ordinance struck down in *Smith v. California*.").
[5] Smith v. California, 361 U.S. 147, 153-54 (1959).

In attempting to avoid the expanded liability under these bills, platforms are likely to scan all user-uploaded content for child sexual abuse material (CSAM). Due to the sheer volume of content they would have to police, they are likely to use automated content tools. These tools would remove more than just CSAM. A broad array of lawful content will inevitably get swept into the net because automated content tools are notoriously both over- and under-inclusive.[6] Nonetheless, for platforms, over-censorship would be preferable to facing expanded legal risk. Such "self-censorship, when compelled by the State, would be a censorship affecting the whole public, hardly less virulent for being privately administered."[7]

We have seen such over-censorship before. After Congress passed SESTA/FOSTA to protect against sex trafficking, some websites instead removed all sex-related content.[8] This problem would be worse under Cooper Davis because, as hard as it is to reliably identify CSAM, it is likely to be far more difficult to identify communications about illegal drug transactions, which are often in code.

Over-censorship is likely to have an outsized impact on LGBTQ+ individuals, sex workers, and reproductive rights activists, who often discuss matters involving sex and sexual education. This is particularly true for LGBTQ+ youth, who seek information and community online, particularly if their friends, family and community do not accept them for who they are.

These Bills Disincentivize Platforms from Protecting User Privacy and Security with Strong Encryption

Moreover, platforms are likely to stop offering private, secure communications tools like end-to-end encryption if faced with expanded liability. Encryption shields the contents of communications from

---

[6] *See* Dhanaraj Thakur & Emma Llansó, Center for Democracy & Technology, Do You See What I See? (2021).
[7] *Smith*, 361 U.S. at 153-54.
[8] Liz Tung, *FOSTA-SESTA Was Supposed to Thwart Sex Trafficking. Instead, It's Sparked a Movement*, WHYY (July 10, 2020), https://whyy.org/segments/fosta-sesta-was-supposed-to-thwart-sex-trafficking- instead-its-sparked-a-movement/; Aja Romano, *A New Law Intended to Curb Sex Trafficking Threatens the Future of the Internet as we Know It*, Vox (July 2, 2018), https://www.vox.com/culture/2018/4/13/ 17172762/fosta-sesta-backpage-230-internet-freedom.

ACLU
AMERICAN CIVIL LIBERTIES UNION

National Political Advocacy Department
915 15th Street, NW, 6th Floor
Washington, DC 20005-2112
aclu.org

Deirdre Schifeling
National Political Director

Anthony D. Romero
Executive Director

Deborah N. Archer
President

outsiders, and is critical for journalists speaking to their sources, doctors talking to their patients, businesses negotiating deals or financial transactions, and anyone else who seeks to keep their communications secure from commercial surveillance, hackers, and, in today's climate, law enforcement investigating reproductive or gender affirming care.

Platforms offering end-to-end encryption could reasonably fear that courts will find merely offering these services is negligent, since their users' encrypted communications are private by design. For example, the EARN IT Act makes explicit that, while encryption cannot be the sole basis for liability, it can be a factor that plaintiffs, juries, and courts can point to in establishing recklessness or negligence.[9]

Disabling end-to-end encrypted services would be disastrous for those who rely on secure, private communications. While this Committee held a hearing to protect a woman's right to have an abortion just last week,[10] it is now considering legislation that would empower prosecutors to access the private online conversations of women seeking reproductive healthcare. Likewise, many members of this Committee have sought to protect individuals identifying as LGBTQ+.[11] However, this year alone, states have introduced 471 anti-LGBTQ+ bills.[12] Just as states could use unencrypted messages as evidence in abortion trials, they could also use unencrypted messages as evidence in trials seeking to criminalize or penalize LGBTQ+ individuals and their doctors.

Expanding Law Enforcement Access to Private Data

ACLU
AMERICAN CIVIL LIBERTIES UNION

National Political Advocacy Department
915 15th Street, NW, 6th Floor
Washington, DC 20005-2112
aclu.org

Deirdre Schifeling
National Political Director

Anthony D. Romero
Executive Director

Deborah N. Archer
President

[9] EARN IT Act, S. 1207, 118th Cong., sec. 5, § 230(e)(7)(B).
[10] U.S. Senate Committee on the Judiciary, *Full Committee Hearing: The Assault on Reproductive Rights in a Post-Dobbs America* (Apr. 26, 2023), *available at* https://www.judiciary.senate.gov/committee-activity/hearings/the-assault-on-reproductive-rights-in-a-post-dobbs-america.
[11] U.S. Senate Committee on the Judiciary, *Press Release: Durbin Praises Senate Advancement of The Respect for Marriage Act* (Nov. 16, 2022), *available at* ,https://www.judiciary.senate.gov/press/dem/releases/durbin-praises-senate-advancement-of-the-respect-for-marriage-act; U.S. Senate Committee on the Judiciary, *Press Release: Durbin, Duckworth Join Brown, Senate Democrats in Introducing Resolution to Recognize June as LGBTQ Pride Month* (June 2, 2022), *available at* https://www.judiciary.senate.gov/press/dem/releases/durbin-duckworth-join-brown-senate-democrats-in-introducing-resolution-to-recognize-june-as-lgbtq-pride-month.
[12] American Civil Liberties Union, Mapping Attacks on LGBTQ Rights in U.S. State Legislatures, *available at* https://www.aclu.org/legislative-attacks-on-lgbtq-rights, (last updated May 2, 2023).

Current law requires platforms to report CSAM that they find on their services to the National Center for Missing and Exploited Children,[13] and allows platforms to report legal offenses to law enforcement if they inadvertently find the evidence.[14] Beyond those circumstances, law enforcement can access user information only through proper legal process, including a warrant.[15] Both the STOP CSAM Act and the Cooper Davis Act, however, would expand mandatory and voluntary reporting by platforms for actual or "apparent" CSAM,[16] and for sales of fentanyl, methamphetamine, or "counterfeit controlled substances."[17] Reports can or must include personal information, such as email address, IP address, geographic information, as well as the contents of communications connected to the known or suspected offense.[18] These laws would get around the warrant requirement and, by doing away with inadvertence, enable the government to pressure platforms to conduct surveillance as arms of the state.

There are other avenues to protect children, privacy, and safety online that do not lead to increased surveillance, censorship and policing. Because these bills would fundamentally alter the free flow of information and make the internet less free, less private, and less secure, we urge you to oppose them. If you have any questions, please don't hesitate to reach out to Jenna Leventoff (JLeventoff@aclu.org), or Cody Venzke (CVenze@aclu.org). Thank you for your attention to this matter.

Sincerely,

Christopher Anders
Federal Policy Director

Jenna Leventoff
Senior Policy Counsel

Cody Venzke
Senior Policy Counsel

ACLU
AMERICAN CIVIL LIBERTIES UNION

National Political Advocacy Department
915 15th Street, NW, 6th Floor
Washington, DC 20005-2112
aclu.org

Deirdre Schifeling
National Political Director

Anthony D. Romero
Executive Director

Deborah N. Archer
President

[13] 18 U.S.C. § 2258A.
[14] 18 U.S.C. § 2702(b)(7).
[15] 18 U.S.C. § 2703(b)(1), (c)(1).
[16] STOP CSAM Act, S. 1199, 118th Cong., sec. 5(a)(1), § 2258A(a).
[17] Cooper Davis Act, S. 1080, 118th Cong, sec. 2(a)(1), § 521(b)(1).
[18] STOP CSAM Act, S. 1199, 118th Cong., sec. 5(a)(1), § 2258A(b); Cooper Davis Act, S. 1080, 118th Cong, sec. 2(a)(1), § 521(c).