May 31, 2023

The Honorable Richard Durbin
Chairman
Senate Committee on the Judiciary
Washington, DC 20510

The Honorable Lindsey Graham
Ranking Member
Senate Committee on the Judiciary
Washington, DC 20510

Re: OPPOSE S. 1080, Cooper Davis Act

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

We write to oppose S. 1080, the Cooper Davis Act.[1] The bill and amendments laudably seek a solution to the proliferation of illegally made fentanyl and resulting overdose deaths in the United States.[2] Unfortunately, even with the proposed manager's amendment, the bill is likely to prove ineffective by sweeping up innocent communications while threatening the privacy of all internet users.

The bill and the manager's amendment would weaken an already insufficient privacy law and would provide a roadmap for more sweeping and overbroad carveouts. Its vague requirements and criminal penalties would result in companies over-reporting users to the Drug Enforcement Administration (DEA) for innocent, protected speech. History shows it may also encourage companies to engage in dragnet scanning of user communications, which would result in even more errors and sweep up the same voices Congress is trying to protect.

The Bill Requires Reporting to the DEA

The bill and the proposed manager's amendment target the "creation, manufacturing, distributing, dispensing, or possession with intent to manufacture, distribute, or dispense" fentanyl, methamphetamine, or a "counterfeit substance." Under the bill, providers shall report to the DEA when they gain actual knowledge of facts or circumstances "indicating an apparent" violation. Providers may make a report if they have a "reasonable belief" about the same information.

Providers have discretion about what to include in a report. But they are encouraged to turn over personal information about the users involved, location information, and their full communications. Providers can face hundreds of thousands of dollars in criminal fines for a failure to report and civil fines for omitting required information in a report.

---

[1] *S.1080, Cooper-Davis Act, 118th Congress,* Congress.Gov (March 30, 2023), *available at* https://www.congress.gov/bill/118th-congress/senate-bill/1080/text?s=1&r=1&q=%7B%22search%22%3A%5B%22Cooper+davis+act%22%5D%7D

[2] *Fentanyl,* Center for Disease Control and Prevention, (June 1, 2022) *available at* https://www.cdc.gov/opioids/basics/fentanyl.html

The DEA can share the information with other federal and state law enforcement agencies.

The proposed language also creates a "request" that providers preserve the report and other relevant information for 90 days with the ability to extend that period (so law enforcement can potentially obtain it later). And it prevents providers from telling their users about the preservation, unless they first notify the DEA and wait 30 days.

The Bill Weakens Privacy And Creates a Template for Further Overbroad Surveillance

This bill creates another carveout in federal privacy protections at a time when these laws desperately need to be strengthened. Under the 1986 Electronic Communications Privacy Act (ECPA), providers are generally restricted from handing over user information to law enforcement without some kind of legal process—whether it be a warrant, court order, or subpoena.[3] Most every state has similar laws, in addition to the federal standard. On multiple occasions in the past seven years, the House of Representatives has overwhelmingly voted to update and strengthen ECPA with broad support from civil society.[4]

S. 1080, both as introduced and in the manager's amendment, unfortunately, goes in the opposite direction. In certain circumstances, it allows providers to hand over identifying information and communications content to the DEA with no judicial review. And while the authors have focused attention on social media[5], this bill would reach far more communications—including private text messages, emails, or even personal files stored in the cloud.

If passed, this will become a template for other legislators to try to force internet companies to report their users to law enforcement for unfavorable conduct or speech, which is a dangerous precedent. Congress appeared to recognize this danger when it refused to apply this same reporting scheme to vaguely defined terror content.[6] The next

---

[3] 18 US. Code §2703, Cornell Law School Legal Information Instititute, *available at* https://www.law.cornell.edu/uscode/text/18/2703

[4] David Ruiz, *Email Privacy Act Comes Back, Hopefully to Stay,* Electronic Frontier Foundation (May, 29, 2018), *available at* https://www.eff.org/deeplinks/2018/05/email-privacy-act-comes-back-hopefully-stay

[5] *Shaheen, Marshall Introduce Bipartisan Bill to Crack Down on Drug Trafficking Through Social Media,* Jeanne Shaheen, U.S. Senator for New Hampshire (March 30, 2023), *available at* https://www.shaheen.senate.gov/news/press/shaheen-marshall-introduce-bipartisan-bill-to-crack-down-on-drug-trafficking-through-social-media

[6] *Coalition Letter Opposing Section 603 of the Intelligence Authorization Act,* Center for Democracy and Technology (August 4, 2015), *available at* https://cdt.org/insights/coalition-letter-opposing-section-603-of-intelligence-authorization-act/; *Letter Opposing Section 602 of the Intelligence Authorization Bill for Fiscal Year 2016*, Internet Association in Internet Archive's Wayback Machine (August 15, 2015), *available at* https://web.archive.org/web/20211217101844/http://internetassociation.org/wp-content/uploads/2015/08/080515-Joint-Letter-on-Section-603.pdf; Mario Trujillo, *Tech Groups Try to Kill*

bill or amendment might target marijuana users, even though non-medical use is legal in more than 20 states.[7] Or new bills might target the sale or purchase of abortion pills, if a new administration deemed those drugs unsafe or illegal for purely political reasons.

This Bill Would Result in Companies Reporting Protected Speech to the DEA

The bill would result in providers reporting their users to the DEA for protected speech, like discussion of past drug use or treatment. The bill's text requires providers to report the facts and circumstances about certain "apparent" drug distribution, manufacture, or possession with intent. But these categories of speech are highly subjective and context dependent. At scale, it will be difficult for providers to find the line between a discussion about past drug use and purchase vs. possession of drugs with intent to distribute. It will be similarly difficult for providers to determine when a conversation discusses an undefined "counterfeit substance"—which has the potential to mean any purported prescription or legal drug. The lack of clarity combined with the threat of large criminal fines will result in overreporting. Providers—and their content moderators who likely lack legal training—are ill-suited to make these determinations, especially when it can result in a government investigation and prosecution of their users.

Even when the reports are accurate, this legislation could result in the investigation and prosecution of the teenage drug users who this law is meant to protect. Congress should not encourage providers to report teens to the DEA. Drug distribution necessarily involves at least two parties (the drug distributor and the drug user). Therefore, reports about drug distribution will inevitably sweep up information about drug users, including teenagers. Congress should carefully think through the unintended consequences of this new internet reporting requirement. People are arrested in the United States for drug possession ahead of nearly any other crime and there remains significant racial disparities in those arrests.[8]

While the data minimization requirements in the amendment are welcome, they remain inadequate. They relate only to storage—not sharing or use—of the reports, and they leave too much discretion in the hands of the DEA to implement "reasonable measures."

Terrorist Reporting Mandate in Spy Bill, The Hill (August 5, 2015), *available at* https://thehill.com/policy/technology/250371-tech-groups-try-to-kill-terrorist-activity-reporting-requirement-in-spy/

[7] *State Medical Cannabis Laws,* National Conference of State Legislatures (April 17, 2023), *available at* https://www.ncsl.org/health/state-medical-cannabis-laws

[8] *Drug Arrests Stay High Even as Imprisonment Fell from 2009 to 2019*, Pew Charitable Trusts (February 15, 2022), *available at* https://www.pewtrusts.org/en/research-and-analysis/issue-briefs/2022/02/drug-arrests-stayed-high-even-as-imprisonment-fell-from-2009-to-2019

This Bill Encourages Dragnet Scanning That Will Inevitably Lead to More Errors

The bill explicitly notes that it does not require providers to scan the content of their users' conversations. But dragnet scanning is completely legal under the bill, and history shows that this type of reporting scheme at least encourages scanning, even if not explicitly required.

The bill is modeled off existing law that requires similar reporting about child sexual abuse material (CSAM), but this bill goes further.[9] Under existing law, providers are required to report actual knowledge of CSAM to a group called the National Center for Missing and Exploited Children, a quasi-governmental entity that later forwards on some reports to law enforcement. Despite strong challenges, the existing CSAM reporting law has so far survived Fourth Amendment scrutiny because the government does not explicitly compel providers to search through their users' communications (it only requires reporting if providers decide to search on their own).[10] However, some applications of existing law have violated the Constitution—specifically, when the government acts on a report where the providers have not fully examined the material they are reporting.[11]

Though not legally required to do so, companies base some of their CSAM reporting on matches found by scanning and comparing digital signatures of images to an existing database of previously removed CSAM.[12]

That kind of content scanning is bound to be ineffective when applied to the search for drug sales and should not be encouraged. While actual CSAM is per se unlawful, mere discussion of drugs is protected and context dependent. And there are no equivalent digital signatures for conversations about drugs remotely similar to the signatures used in the CSAM context. Any company that would purport to offer an accurate scanning tool for conversations about drugs should be viewed with heavy skepticism. For example, if providers started scanning and screening user communications based on the DEA's "Emoji Drug Code Decoded" graphic,[13] any person who sent a cookie emoji or maple

[9] The Cooper Davis Act goes further than the CSAM reporting law in significant ways: (1) it requires reporting about speech that is not per se unlawful; (2) it requires reporting directly to law enforcement; (3) it includes more coercive criminal penalties.
[10] District Judge William Q. Hayes, *Appeal from the United States District Court for the Southern District of Califonria on US v Carlos Senta*, United States Court of Appeals for the Ninth Circuit (October 3, 2022), *available at* https://cdn.ca9.uscourts.gov/datastore/opinions/2022/10/03/20-50052.pdf
[11] Jennifer Lynch, *In U.S. v Wilson, the Ninth Circuit Reaffirms Fourth Amendment Protection for Electronic Communications,* Electronic Frontier Foundation (September 28, 2021), *available at* https://www.eff.org/deeplinks/2021/09/us-v-wilson-ninth-circuit-reaffirms-fourth-amendment-protection-electronic
[12] *PhotoDNA*, Microsoft, *available at* https://www.microsoft.com/en-us/photodna
[13] *Emoji Drug Code, Decoded*, Drug Enforcement Administration, *available at* https://www.dea.gov/sites/default/files/2022-04/Emoji%20Decoded_FO%20One%20Page_v2.pdf

leaf emoji, even if not in a clearly drug related context, would risk having their information sent to the DEA.

The manager's amendment makes clear dragnet scanning using automated tools is one of the anticipated outcomes of the bill. It requires providers to note whether the report originated from a "non-human method including but not limited to use of an algorithm, machine learning or other means." We are also concerned that liability can hinge on a provider who "deliberately blind[s] itself" to a violation. Read broadly, this may be interpreted to sweep up providers who do not—or cannot due to their own security measures—scan user communications.

Other Concerns about Preservation and Notice to Users

Under this bill, providers are asked to preserve content for 90 days with the option for extensions. But there is increasing recognition that this compelled preservation constitutes a Fourth Amendment seizure that removes a user's rights to delete their own content.[14] At minimum, the bill should require the government to get a warrant for the lengthy preservation of content associated with a report.

The bill also prevents providers from telling their users about preservation, unless providers first notify the DEA and wait 30 days. Instead, the bill should make it easier for companies to notify their users about preservation requests, similar to the NDO Fairness Act.[15] This would give users the option to exercise rights over their own information.

For these reasons, we urge Congress to reject this bill, as it did the previous attempt to undermine the privacy of innocent Americans. Congress should be highly skeptical about giving law enforcement broad access to our conversations without judicial oversight. This bill contains no warrant requirement, no required notice, and limited user protections. We urge Congress to vote No.

---

[14] Orin S. Kerr, *The Fourth Amendment Limits of Internet Content Preservation*, Saint Louis University Law Journal (August 2021), *available at* https://scholarship.law.slu.edu/cgi/viewcontent.cgi?article=2264&context=lj

[15] *H.R. 3089, NDO Fairness Act, 118th Congress,* Congress.Gov (May 16, 2023), *available at* https://www.congress.gov/bill/118th-congress/house-bill/3089/text; India McKinney and Naomi Gilens, *The NDO Fairness Act Is an Important Step Towards Transparency,* Electronic Frontier Foundation (April 4, 2022), *available at* https://www.eff.org/deeplinks/2022/04/ndo-fairness-act-important-step-towards-transparency

If you have questions or need additional information, please contact India McKinney at the Electronic Frontier Foundation at india@eff.org.

Signed,

Electronic Frontier Foundation
Advocacy for Principled Action in Government
American Civil Liberties Union
Center for Democracy & Technology
Chamber of Progress
Defending Rights & Dissent
Fight for the Future
Freedom of the Press Foundation
Government Information Watch
National Association of Criminal Defense Lawyers
R Street Institute
S.T.O.P. - Surveillance Technology Oversight Project