March 9, 2020

RE: Oppose the Eliminating Abusive and Rampant Neglect of Interactive Technologies Act of 2020 (EARN It Act)

Dear Senators,

The American Civil Liberties Union, on behalf of its members, writes to express our strong opposition to S. 3398, the Eliminating Abusive and Rampant Neglect of Interactive Technologies Act of 2020 (EARN It Act).[1] The bill undermines the privacy of every single American, stifles our ability to communicate freely online, and may jeopardize the very prosecutions it seeks to enable. We urge the Senate Judiciary Committee to refrain from taking any further action on the EARN It Act and to consider more narrowly tailored approaches to combating the legitimate and serious issues the EARN It Act seeks to address.

AMERICAN CIVIL LIBERTIES UNION

National Political Advocacy Department
915 15th St. NW, 6th FL
Washington, D.C. 20005
aclu.org

Susan Herman
President

Anthony Romero
Executive Director

Ronald Newman
National Political Director

The EARN It Act

The EARN It Act would create a National Commission on Online Child Sexual Exploitation Prevention and it would put the Attorney General at the head of it. The Commission would write best practices for online platforms to "prevent, reduce, and respond to online sexual exploitation of children, including the enticement, grooming, sex trafficking, and sexual abuse of children and proliferation of online child sexual abuse material." The practices must include, among many other things, methods for "preventing, identifying, disrupting, and reporting child sexual exploitation," retaining information related to it and reporting it to law enforcement, categorizing and rating the material, and implementing age gating and age rating practices.

After the Commission fills in the details of the best practices, the AG, upon agreement with the heads of the FTC and DHS, would have veto power over the practices. This means the best practices will overwhelmingly reflect the preferences of whoever is AG at the time the best practices are submitted and, because the practices will need to be updated every five years, they could change based upon the preferences of the individual in the AG's office. After the AG approves, both Houses of Congress would have to vote, under expedited processes, to enact the best practices.

Once Congress enacts the best practices, online companies will have a "choice" that is really no choice at all. Platforms could "choose" to comply with the best practices and submit a certification to that effect to the AG. If they do so, they will retain protections from civil and state criminal liability under Section 230 of the Communications Decency Act for hosting child sexual abuse material ("CSAM")

provided by users on their services. However, this carrot is not without its stick. If a company files a certification that the AG determines to be false, the company may face criminal penalties.

Platforms could also, theoretically, choose not to certify compliance with the best practices. If they go this route, they will lose the protection of Section 230 of the CDA for CSAM on their services, unless a judge determines that their practices for combatting child sexual exploitation are reasonable in reference to the best practices the Commission would develop. To make matters worse, the bill would lower the mens rea standard applicable to publishing third-party content that is CSAM from actual knowledge to reckless disregard. Absent 230's protections, platforms could be on the hook for all CSAM that travels over their services under the theory that they reasonably know their services are being used that way and are not preventing that use, regardless whether such prevention is possible.

Though it purports to address some of society's worst crimes, in reality, the EARN It Act will do far more harm than good. It will jeopardize the privacy of every American, fundamentally alter the freedom of our online communications, and, potentially, undermine the very prosecutions it seeks to enable.

The EARN It Act Harms Our Privacy and Security.

Encrypted communications are vital to everyone's privacy. They help ensure the safety of domestic violence victims from their abusers.[2] They shield dissidents and journalists in the U.S. and abroad from the prying eyes of their governments.[3] They protect Members of Congress from malicious surveillance by foreign actors.[4] The 82nd Airborne, deployed in the Middle East, uses Signal and Wickr, commercially available encrypted applications, to avoid surveillance by the Iranian government.[5] In the same way they protect Members of the Senate Judiciary Committee and the 82nd Airborne, encrypted services protect all of us from the prying eyes of hostile foreign governments and numerous other bad actors.

---

[1] S. 3398, 116th Cong., 2d Sess. (2020). We further note that we join at least twenty-five other civil society groups in opposing this bill. *See* Letter to Senator Lindsey Graham and Senator Richard Blumenthal from the Open Technology Institute & Twenty-Four Organizations Opposing the EARN It Act (Mar. 6, 2020), https://newamericadotorg.s3.amazonaws.com/documents/Coalition_letter_opposing_EARN_IT_3-6-20.pdf.

[2] Hoa Nguyen, *Encryption Backdoors Put More At Risk Than You Might Think*, OPEN TECH. INST. (Dec. 13, 2018), https://www.newamerica.org/weekly/encryption-backdoors-put-more-risk-you-might-think/; Kaefong Lee, *Smartphone Encryption: Protecting Victim Privacy While Holding Offenders Accountable*, NAT'L NETWORK TO END DOMESTIC VIOLENCE (Apr. 12, 2016). https://www.techsafety.org/blog/2016/4/12/smartphone-encryption-protecting-victim-privacy-while-holding-offenders-accountable/

[3] See, e.g., Francesca Ebel, *Outlawed app emerges as key tool for Russian protesters*, ASSOC. PRESS (Sept. 6, 2019), https://apnews.com/34df8b282f6c4fd188a33d2fb3ff381c; Fion Lee, Blake Schmidt, Shawna Kan, Tracy Alloway, *How Encrypted Messages and Car 'Crashes' Helped Hong Kong Protesters*, BLOOMBERG (June 13, 2019), https://www.bloomberg.com/news/articles/2019-06-13/how-encrypted-messages-car-crashes-helped-hong-kong-protesters; Spencer Woodman, *Five Digital Security Tools Journalists Use to Protect Their Work and Sources,* INTERNAT'L CONSORTIUM OF INVESTIGATIVE JOURNALISTS (Jan. 29, 2018), https://www.icij.org/blog/2018/01/five-digital-security-tools-to-protect-your-work-and-sources/.

[4] Joe Uchill, *Senate approves encrypted app Signal for staff use*, THE HILL (May 17, 2017), https://thehill.com/policy/cybersecurity/333802-sen-staff-can-use-signal-for-encrypted-chat.

[5] Shawn Snow, Kyle Rempfer, & Meghann Myers, *Deployed 82nd Airborne Unit Told to Use These Encrypted Apps on Government Cell Phones*, MILITARY TIMES (Jan. 23, 2020), https://www.militarytimes.com/flashpoints/2020/01/23/deployed-82nd-airborne-unit-told-to-use-these-encrypted-messaging-apps-on-government-cellphones/.

The EARN It Act jeopardizes those essential services. The best practices would require companies to develop methods for identifying, retaining, and reporting "child sexual exploitation" on their services. When designing the best practices, the Commission must consider "the impact on the ability of law enforcement agencies to investigate and prosecute child sexual exploitation and rescue victims." Attorney General William Bar has identified end-to-end encryption as one of the primary obstacles to law enforcement investigations related to CSAM and other crimes.[6] It stands to reason that a Commission, with Attorney General Barr at the head and a number of members that are law enforcement, will decide that refraining from deploying end-to-end encryption, building in "back doors", or otherwise enabling communications surveillance are a "best practice" for "combating child sexual exploitation." Back doors and other vulnerabilities in encrypted services are open doors to criminals and hostile foreign governments.[7] There is no way to ensure that only law enforcement could exploit the vulnerabilities these best practices could force platforms to build in to their services.[8]
Furthermore, even if a platform were to decline to follow the best practices and deploy end-to-end encryption, the platform would then risk lawsuits claiming that deploying end-to-end encryption, itself, is reckless conduct now subject to civil liability under the EARN It Act. Claimants could argue the platform recklessly protected against accessing contents of communications although the platform was reasonably aware that its systems were used to distribute illegal CSAM.

Whichever path platforms choose under the EARN It Act, the privacy of our communications are at risk.

The EARN It Act Is a Tool for Censorship.

The EARN It Act will also chill vast amounts of protected speech online in two general ways. First, by undermining the privacy of communications, vulnerable people will not communicate freely. Protesters, domestic violence victims, and others that use encrypted communications to maintain safety will be afraid to speak if the EARN It Act becomes law. Second, the EARN It Act harms free speech by essentially mandating companies adopt overbroad content censorship and moderation practices.

The best practices the bill outlines will address prevention, reduction and responses to "online sexual exploitation of children, including the enticement, grooming, sex trafficking, and sexual abuse of children, and the proliferation of child sexual abuse material." To address these broadly defined dangers, the best practices must include content moderation practices, plans to maintain information about all of these various potential dangers and

---

[6] Attorney General William P. Barr, Keynote address at the International Conference on Cybersecurity (July 23, 2019), https://www.justice.gov/opa/speech/attorney-general-william-p-barr-delivers-keynote-address-international-conference-cyber.
[7] *See* Susan Landau, *If We Build It (They Will Break In)*, LAWFARE (Feb. 28, 2020), https://www.lawfareblog.com/if-we-build-it-they-will-break; Open Technology Institute, *Encryption Backdoors Are a Dangerous Idea* (Nov. 27, 2018), https://www.newamerica.org/oti/blog/encryption-backdoors-are-dangerous-idea/.
[8] Michael Hayden, *Encryption Backdoors Won't Stop Crime But Will Hurt U.S. Tech.*, BLOOMBERG (Dec. 10, 2019), https://www.bloomberg.com/opinion/articles/2019-12-10/encryption-backdoors-won-t-stop-crime-but-will-hurt-u-s-tech.

report them to law enforcement, implementation of a rating and categorization system for "child sexual exploitation material" and employment of age gating and age rating.

The aftermath of the passage of SESTA/FOSTA,[9] which eliminated Section 230's liability shield for content related to sex trafficking, has taught us a lesson.[10] Even if the speech covered by the law can be restricted without raising constitutional concern, the content moderation practices the companies will deploy to avoid liability risk will sweep far more broadly than the illegal content.[11] SESTA/FOSTA was intended to protect women engaged in sex work from being trafficked against their will. It has, instead, sent them back out into the streets and made them less safe.[12] Moreover, the platforms' content moderation practices have disproportionately silenced the LGBTQ+ community, making it more difficult for them to come together and create community online.[13]

The EARN It Act presents similar risks. There are myriad ways in which adults communicate normally and healthily with children online that could be swept up in the content moderation practices the EARN It Act would require platforms to adopt. Any communication between a teacher and their students or an aunt or uncle with their nieces and nephews could be suppressed or censored by the best practices. That is an unacceptably speech-chilling solution to a problem that could be solved with a far more narrowly tailored measure.

Speech-chilling concerns aside, the EARN It Act may also be unconstitutional. Established precedent indicates the government cannot coerce private actors into engaging in censorship the government cannot compel on its own.[14] Despite this clear prohibition, the EARN It Act coerces platforms into censoring speech that will go well beyond illegal CSAM. The constitutional implications are inescapable and raise questions regarding the EARN It Act's effectiveness in protecting children.

---

[9] Allow States and Victims to Fight Online Sex Trafficking Act of 2017, Pub. L. 115-164 (2018), *available at* https://www.congress.gov/bill/115th-congress/house-bill/1865.
[10] Ian S. Thompson, *Congress Proposes to Fight Online Sex Trafficking by Harming Sex Workers*, ACLU (Mar. 16, 2018), https://www.aclu.org/blog/criminal-law-reform/congress-proposes-fight-online-trafficking-harming-sex-workers.
[11] Daniel Villareal, *SESTA/FOSTA Is Turning the Web into a G-Rated Minefield*, LGBTQNATION (Mar. 16, 2019), https://www.lgbtqnation.com/2019/03/sesta-fosta-turning-web-g-rated-minefield-dan-savage-pals-know-2-ways-destroy/; Michael Aaron, *Why FOSTA/SESTA Harms Those it Supposedly Serves*, PSYCHOLOGY TODAY (Jul. 17, 2018), https://www.psychologytoday.com/us/blog/standard-deviations/201807/why-fostasesta-harms-those-it-supposedly-serves.
[12] Makena Kelly, *Democrats Want Data on How Sex Workers Were Hurt by Online Crackdown*, THE VERGE (Dec. 17, 2019), https://www.theverge.com/2019/12/17/21026787/sesta-fosta-congress-study-hhs-sex-work-ro-khanna-elizabeth-warren-ron-wyden.
[13] Alexander Cheeves, *The Dangerous Trend of LGBTQ Censorship on the Internet*, OUT MAGAZINE (Dec. 6, 2018), https://www.out.com/out-exclusives/2018/12/06/dangerous-trend-lgbtq-censorship-internet.
[14] *See* Bantam Books, Inc. v. Sullivan, 372 U.S. 58 (1963) (invalidating a government Commission that notified book distributors when the Commission considered certain books to be objectionable because it was a "scheme of state censorship"); Backpage.com LLC v. Dart, 807 F. 3d 229 (7th Cir. 2015) (holding that law enforcement violated the First Amendment when it pressured Visa and Mastercard to cease doing business with Backpage because law enforcement had "threatened imposition of government power or sanction" in order to stifle speech).

The EARN It Act is Counterproductive.

Finally, the EARN It Act counterproductively risks harming law enforcement's ability to bring child predators to justice. Currently, online platforms are required to report CSAM to NCMEC when they become aware of the material on their platforms but they are not required to go looking for it.[15] The EARN IT Act intends to require platforms to do far more.

The government cannot circumvent the requirements of the Fourth Amendment by deputizing others to conduct searches on its behalf.[16] A Tenth Circuit case, written by then-Judge Neil Gorsuch, applied this principle when it found the National Center for Missing and Exploited Children (NCMEC) to be either a government entity or acting as an agent of the government when opening a suspect's email to investigate a CSAM report.[17] NCMEC's investigation was therefore subject to the restrictions of the Fourth Amendment.

The EARN It Act is clearly intended to develop affirmative investigatory steps to identify CSAM and essentially require providers to conduct that investigation. It deputizes private parties to do an investigation on behalf of law enforcement, requires preservation of the evidence and reporting to law enforcement. Failure to comply means the loss of an important liability shield, as well as imposition of civil liability at a much lower threshold than current law would apply. Given the government's extensive involvement in creating the standards for the searches and instigating them to aid its own purposes, there are strong arguments that platform providers will be agents of the government for Fourth Amendment purposes under the EARN It Act at least in some instances. For example, when analyzing whether a private party is acting as an agent of the government, the First Circuit examines (1) ""the extent of the government's role in instigating or participating in the search"; (2) "[the government's] intent and the degree of control it exercises over the search and the private party"; and (3) "the extent to which the private party aims primarily to help the government or to serve its own interests."[18] Any evidence of CSAM obtained through investigations conducted to comply with the EARN It Act therefore could be inadmissible in court if obtained without a warrant or in any other manner that does not comply with the Fourth Amendment.

Supporters of the bill have argued that the EARN It Act will likely not result in suppression of evidence.[19] Specifically, they claim that "when a company has terms and conditions that enable it to privately search, there is no Fourth Amendment violation

---

[15] 18 U.S.C. 2558A.
[16] *See* Skinner v. Ry. Labor Execs.' Ass'n., 489 U.S. 602, 614 (1989(("Although the Fourth Amendment does not apply to a search or seizure, even an arbitrary one, effected by a private party on his own initiative, the Amendment protects against such intrusions if the private party acted as an instrument or agency of the government.").
[17] U.S. v. Ackerman, 831 F. 3d 1292 (10th Cir. 2016). *See also*, United States v. Keith, 980 F.Supp.2d 33 (D. Mass. 2013); United States v. Tolbert, 326 F.Supp.3d 1211 (D. New Mexico 2018).
[18] U.S. v. Silva, 554 F.3d 13, 18 (1st Cir. 2009). There are different tests employed in the various circuits, but each asks whether a private actor is acting at government behest and with the intention of assisting law enforcement. *See* Jeff Kosseff, *Private Computer Searches and the Fourth Amendment*, 14 I/S: A J. OF L. & POLICY 187 (2018), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3225742.
[19] The EARN It Act: Concerns and Responses, https://techfreedom.org/wp-content/uploads/2020/03/EARN-IT-Concerns-and-Responses-2-28.pdf.

because users lose their reasonable expectation of privacy."[20] In *United States v. Carpenter*, a case the ACLU argued, the Supreme Court held that warrantless searches of cell-site records violate the Fourth Amendment.[21] *Carpenter* holds that our sensitive information does not lose Fourth Amendment protection merely because we store that information on a "third-party" server.[22] Terms of service do not eliminate our expectation of privacy in our communications.[23] Indeed, the Supreme Court recently made clear that contractual terms do not automatically determine Fourth Amendment rights.[24]

Supporters also posit that there might be no Fourth Amendment problem with making scanning for CSAM a best practices because "courts might find that just as DWI checkpoints or dog-sniff tests are reasonable under the Fourth Amendment, so is a requirement that companies utilize non-invasive technological mechanisms for identifying the most heinous criminal content."[25] To begin, these technologies must check every file that traverses a service. They are therefore deeply invasive. More importantly, this argument pretends that every scan for CSAM will be treated similarly under the Fourth Amendment. That is simply not true. Dog sniffs are not permitted at all times in all circumstances. It is not reasonable, for instance, to bring a dog onto the porch of someone's home.[26] At best, the constitutionality of government-agent searches for CSAM is context-dependent. Even accepting supporters' arguments, there will be cases in which clear evidence of CSAM is suppressed because the search that produced it was unconstitutional and that will be the direct result of the EARN It Act.

The EARN It Act is undoubtedly well-intentioned and seeks the legitimate and worthy goal of protecting children from real dangers. However, it is not the solution to the problems it claims to address. One possible more effective way to protect and defend children from the online dangers they face would be to better equip law enforcement agencies to respond. We urge the Committee to refrain from taking any additional action on the EARN It Act and to consider adopting a different approach to these serious problems. Please contact Kate Ruane, kruane@aclu.org, (202) 675.2336, with any questions.

Sincerely,

Ronald Newman
National Political Director

Kate Ruane
Senior Legislative Counsel

---

[20] *Id*.
[21] Carpenter v. United States, 585 U.S. ___, 138 S. Ct. 2207, 2217 (2018).
[22] Nathan Freed Wessler, *The Supreme Court's Most Consequential Ruling for Privacy: One Year In*, ACLU (Jun 18, 2019), https://www.aclu.org/blog/privacy-technology/location-tracking/supreme-courts-most-consequential-ruling-privacy-digital.
[23] In *Carpenter*, every Justice agreed, at least in dicta, that the Fourth Amendment protects the content of emails stored on a third-party service. See 138 S. Ct. at 2222 (majority op.); id. at 2230 (Kennedy, J., dissenting, joined by Thomas and Alito, JJ.); id. at 2262, 2269 (Gorsuch, J., dissenting).
[24] Byrd v. United States, 138 S. Ct. 1518 (2018) (holding that a person retains Fourth Amendment rights in a rental car even if they are not the permitted driver under the rental agreement).
[25] The EARN It Act: Concerns and Responses, https://techfreedom.org/wp-content/uploads/2020/03/EARN-IT-Concerns-and-Responses-2-28.pdf.
[26] Florida v. Jardines, 569 U.S. 1 (2013).