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

June 29, 2020

Re: Vote "NO" on 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, opposes S. 3398, the Eliminating Abusive and Rampant Neglect of Interactive Technologies Act of 2020 (EARN IT Act).[1] At this extraordinary time, while Congress has neglected its responsibility to address the global pandemic, ongoing economic crisis, and the calls for change demanded by unprecedented protests for racial justice, it is disappointing that the Committee is choosing to advance legislation that undermines the privacy of every single American, stifles our ability to communicate freely online, harms LGBTQ people, sex workers, and protesters, and jeopardizes the very prosecutions it seeks to enable.

We urge you to vote "NO" on passage of the EARN IT Act out of the Senate Judiciary Committee. The ACLU will score this vote.

The ACLU has consistently supported efforts to ensure that those who experience sexual abuse, especially children, are not afraid to come forward, and that when they do, they are treated fairly and equitably. While the stated goals of the EARN IT Act to protect children from online child sexual exploitation are laudable, it fails to meaningfully solve the problem it purports to address. For example, the bill fails to do anything at all to address the root causes of child sexual exploitation in order to prevent children from ever falling victim in the first place. It also completely fails to provide any assistance for victims to receive support, care, and counseling to mitigate harms caused by traumatic events or any protections from the potential immigration, criminal, or other negative consequences of coming forward to report crimes against them. The bill will do nothing to solve these fundamental problems, while creating a multitude of other ones.

Rather than protect children from harm, the EARN IT Act instead would harm the privacy and online speech rights of every person in this country. By amending a key federal law that supports online speech, it also will disproportionately harm the LGBTQ community and sex worker community in ways similar to SESTA/FOSTA, a law that changed the same provision in 2018. SESTA/FOSTA was intended to protect people engaged in sex work from being trafficked against their will. However, sex workers use online platforms to screen potentially violent clients, share information regarding health and safety, and otherwise communicate privately and safely. SESTA/FOSTA eliminated many of the spaces sex workers used to

maintain safety and protect their health and sent sex worker back out into the streets into dangerous situations. Rather than protecting people from illegal trafficking, SESTA/FOSTA jeopardized the health, safety, and welfare even further than it had been. Rep. Khanna has introduced legislation that the ACLU supports calling for a federal study to quantify this harm. Furthermore, SESTA/FOSTA also caused disproportionate censorship of the speech of LGBTQ people online as well.

The EARN IT Act would be even more dangerous than SESTA/FOSTA. It would harm the privacy and online expression of every person and will disproportionately harm LGBTQ communities, protesters, and other marginalized communities. And for sex workers, who are among our most vulnerable communities, the impacts would be even more dire and could place their lives at risk. This is unacceptable.

We urge Senate Judiciary Committee Members to vote NO on the EARN IT Act to stop this dangerous legislation from further consideration. The ACLU will score this vote.

The EARN IT Act would create a National Commission on Online Child Sexual Exploitation Prevention and it would put the Attorney General or his representative at the head of it. It would then task this unelected Commission with writing 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 Commission would not include representation from the LGBT, sex worker, or other marginalized communities, ensuring the concerns of impacted communities would not be considered in the development of the best practices. Under the bill, the best practices developed by the Commission would have to 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 filled 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 would overwhelmingly reflect the preferences of whoever is AG at the time the best practices are submitted and, because the practices would 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, with little opportunity for debate or amendment.

Once Congress enacted the best practices, online companies would 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 did so, they would retain protections from civil and state criminal liability under Section 230 of the Communications Decency

---

[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.

Act for hosting child sexual abuse material ("CSAM") provided by users on their services. However, this carrot would not be without its stick. If a company filed a certification that the AG determined to be false, the company could face criminal penalties. And, any company could face a broad administrative subpoena requesting any material that is relevant to such a certification or testimony about such material.

Platforms could also, theoretically, choose not to certify compliance with the best practices. If they went this route, they would lose the protection of Section 230 of the CDA for CSAM provided by others on their services, unless a judge determines that their practices for combatting child sexual exploitation were reasonable in reference to the best practices the Commission had developed. To make matters worse, the bill would lower the mens rea standard applicable to publishing third-party CSAM content 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 to spread such content and are not preventing that use, regardless of whether such prevention is even 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, disproportionately harm LGBTQ people, sex workers, and those with marginalized or minority views, and, potentially, undermine the very prosecutions it claims to enable.

The EARN IT Act Harms Our Privacy and Security.

The EARNT IT Act grants broad authority to an unelected Commission to write best practices that will likely encourage platforms to undermine strong encryption methods and place our online privacy at risk. Encrypted communications are vital to everyone's privacy and safety. Amidst the recent historic protests for racial justice after the murders of George Floyd, Breonna Taylor, Rayshard Brooks, and so many others at the hands of police, many protesters used encrypted applications to communicate with each other to guard against the prying eyes of law enforcement.[2] Strong encryption is vital to many in the LGBTQ community who rely on the internet to access a support network; seek resources to combat discrimination and abuse; and find doctors and treatment to assist with transition and other health concerns. Encrypted applications help ensure the safety of domestic violence victims from their abusers.[3] They shield dissidents and journalists in the U.S. and abroad from the prying eyes of repressive governments – and indeed the State Department has supported the development and use of encryption for these purposes.[4] They protect

---

[2] Amelia Nierenberg, *Signal Downloads are Way Up Since the Protests Began*, NY TIMES (Jun. 11, 2020), https://www.nytimes.com/2020/06/11/style/signal-messaging-app-encryption-protests.html.

[3] 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/

[4] 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),

Members of Congress from malicious surveillance by foreign actors.[5] The 82nd Airborne, deployed in the Middle East, uses Signal and Wickr, commercially available encrypted applications, to avoid surveillance by the Iranian government.[6]

Back doors and other vulnerabilities in encrypted services are open doors to criminals and hostile foreign governments.[7] As cybersecurity experts have emphasized, there is no way to ensure that only law enforcement could exploit the vulnerabilities the EARN IT Act Commission's best practices could force platforms to build in to their services.[8] Even more, when companies weaken encryption for U.S. consumers, they are poorly positioned to resist requests by foreign governments to apply the same standards to products abroad. This can pose a particular threat to individuals abroad that live in countries that actively persecute and criminalize LBGTQ people as well as any dissenting voices.

The EARN IT Act jeopardizes those essential encrypted 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 would be required to consider "the impact on the ability of law enforcement agencies to investigate and prosecute child sexual exploitation and rescue victims." AG Barr has identified end-to-end encryption as one of the primary obstacles to law enforcement investigations related to CSAM and other crimes.[9] 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."

Furthermore, even if a platform were to decline to follow the best practices and deploy end-to-end encryption in spite of them, 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.

In addition, this would have a disproportionately negative impact on small businesses. Large corporations would likely have the expertise and resources to defend against a suit

---

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/.

[5] 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.

[6] 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/.

[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.

[9] 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.

claiming they are liable under the new standards in the EARN IT Act. Small businesses, on the other hand, would likely lack such capacity. Thus, they would potentially have to choose between the risk of a lawsuit or a loss of competitiveness stemming from adoption of practices that decrease the cybersecurity of their products. Whichever path platforms chose under the EARN IT Act would place the privacy of our communications at risk.

The EARN IT Act Is a Tool for Censorship.

The EARN IT Act would also chill vast amounts of protected speech online in two general ways. First, by undermining the privacy of communications, it would chill vulnerable people from communicating freely. LGBTQ people, protesters, domestic violence victims, sex workers, 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 would harm free speech by essentially mandating companies adopt overbroad content censorship and moderation practices which would disproportionately result in the censorship of LGBTQ voices and the speech of sex workers.

The best practices the bill outlines would 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." As an initial matter, it is worth noting that speech that facilitates crimes against children is illegal, and those who engage in it can be punished. But the content moderation practices the best practices would require would sweep far more broadly than that to include a great deal of constitutional and valuable speech engaged in by or directed to children. For instance, the requirement for best practices to include "age gating" and "age rating", relate solely to children's ability to access content; they have nothing to do with reducing exploitation and everything to do with censoring and restricting legal content. Furthermore, the composition of the Commission would not include representation of impacted communities like sex workers and the LGBTQ community, ensuring that the best practices would not reflect their interests or alleviate their concerns.

The aftermath of the passage of SESTA/FOSTA,[10] which eliminated Section 230's liability shield for content related to sex trafficking, makes the overbroad implications for online speech clear.[11] Even if the speech covered by the law could 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.[12] SESTA/FOSTA was intended to protect women engaged in sex work from being trafficked against their will. It

---

[10] 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.
[11] 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.
[12] 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.

has, instead, sent them back out into the streets and made them less safe.[13] 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.[14]

The EARN IT Act presents even graver risks, especially for the LGBTQ and sex worker communities. By requiring platforms to broadly monitor and censor speech to which children might be exposed online, the EARN IT Act's Commission may recommend best practices that disproportionately censor, among other things: sex education materials, online support systems and communities for youth who are transgender or non-binary or have experienced sexual assault, and all other youth who are in any way questioning their gender or sexual identity, any sex-related speech, the speech of sex workers and of those in the sex industry, and any communication or speech involving youth. Paradoxically, the best practices could harm children's ability to engage fully and experience the tremendous benefits to education and enrichment the Internet offers. It may also interfere with the ability of children who have experience child sexual exploitation to turn to the Internet for community, support, and information. 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.[15] Despite this clear prohibition, the EARN IT Act would coerce 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.

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.[16] 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.[17] A Tenth Circuit case, written by then-

---

[13] 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.

[14] 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.

[15] *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).

[16] 18 U.S.C. 2558A.

[17] *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.").

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.[18] 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, and 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."[19] 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.[20] Specifically, they claim that "when a company has terms and conditions that enable it to privately search, there is no Fourth Amendment violation because users lose their reasonable expectation of privacy."[21] 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.[22] *Carpenter* holds that our sensitive information does not lose Fourth Amendment protection merely because we store that information on a "third-party" server.[23] Terms of service do not eliminate our expectation of privacy in our communications.[24] Indeed, the Supreme Court recently made clear that contractual terms do not automatically determine Fourth Amendment rights.[25]

---

[18] U.S. v. Ackerman, 831 F. 3d 1292 (10th Cir. 2016).
[19] 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.
[20] The EARN IT Act: Concerns and Responses, https://techfreedom.org/wp-content/uploads/2020/03/EARN-IT-Concerns-and-Responses-2-28.pdf.
[21] *Id*.
[22] Carpenter v. United States, 585 U.S. ___, 138 S. Ct. 2207, 2217 (2018).
[23] 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.
[24] 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).
[25] 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).

Supporters also posit that there might be no Fourth Amendment problem with making scanning for CSAM a best practice 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."[26] 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.[27] 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 when those perpetrators walk free they will have the EARN IT Act to thank.

The EARN IT Act seeks to accomplish the legitimate and worthy goal of protecting children from real dangers. However, it is not the solution to the problems it claims to address. Instead, the EARN IT Act will undermine privacy in ways that harm protesters at a time when Congress should be doing everything in its power to ensure their protection. The EARN IT Act will also disproportionately harm the LGBTQ and sex worker communities by overcensoring their speech and undermining the private communications services that are vital to their health, safety and well-being. We urge you to vote NO on passage of the EARN IT Act out of the Senate Judiciary Committee. Please contact Kate Ruane, kruane@aclu.org, (202) 675.2336, Neema Singh Guliani, nguliani@aclu.org, or Ian Thompson, ithompson@aclu.org, with any questions.

Sincerely,

Ronald Newman
National Political Director

Kate Ruane
Senior Legislative Counsel

Neema Singh Guliani
Senior Legislative Counsel

Ian Thompson
Senior Legislative Representative

---

[26] The EARN IT Act: Concerns and Responses, https://techfreedom.org/wp-content/uploads/2020/03/EARN-IT-Concerns-and-Responses-2-28.pdf.
[27] Florida v. Jardines, 569 U.S. 1 (2013).