The Unconstitutional, Unworkable EARN IT Act

by Berin Szóka[1]

The "crypto wars" have broken out again. As in the early 1990s, law enforcement wants backdoor access to Americans' private communications. Just as Communications Assistance for Law Enforcement Act (CALEA) of 1994[2] required backdoors for telecom services, one pending bill would impose equivalent "capability to assist" requirements on Internet services.[3] This would ban end-to-end ("strong") encryption. Such a direct prohibition remains unlikely to pass: this bill remains a purely Republican effort. But the same goal can be achieved indirectly. The Eliminating Abusive and Rampant Neglect of Interactive Technologies Act (EARN IT) of 2020, is clearly modeled on the Stop Enabling Sex Traffickers Act (SESTA) of 2017, which sailed through Congress with little opposition. Introduced by Lindsay Graham (R-SC) and Richard Blumenthal (D-CT), the bill already has the support of six Democratic Senators and five Republicans.[4] President Trump's Department of Justice came out in support of the bill in mid-June, proposing to crack down on "bad actors who … are willfully blind to criminal content on their own services."[5]

In fact, DOJ has pushed for restrictions on online encryption for years. In 2014, James Comey, then Director of the FBI, gave a major address lamenting the "the challenge of going dark": "Those charged with protecting our people aren't always able to access the evidence we need to prosecute crime and prevent terrorism even with lawful authority. We have the legal authority to intercept and access communications and information pursuant to court order,

---

[1] The author of this article, Berin Szóka (bszoka@techfreedom.org), is a Senior Fellow at, and founder of, TechFreedom, a non-profit, non-partisan technology policy think tank.

[2] The Communications Assistance for Law Enforcement Act (CALEA, P.L. 103- 414, 47 USC 1001-1010), enacted October 25, 1994.

[3] Lawful Access to Encrypted Data Act, S. __, 116th Cong. (2020) *available at* https://techfreedom.org/wp-content/uploads/2020/06/OLL20597.pdf.

[4] Eliminating Abusive and Rampant Neglect of Interactive Technologies Act of 2020, S. 3398, 116th Cong. (2020) [hereinafter the *EARN IT Act*].

[5] Press Release, *Justice Department Issues Recommendations for Section 230 Reform*, Dep't of Justice (June 17, 2020,) https://www.justice.gov/opa/pr/justice-department-issues-recommendations-section-230-reform.

but we often lack the technical ability to do so."[6] The FBI kept up a steady drumbeat on this topic through 2016,[7] but with Comey's departure in May of 2017, the cause lost focus. This February, the DOJ held a workshop entitled: "Section 230 – Nurturing Innovation or Fostering Unaccountability?"[8] The workshop's title made clear the DOJ's agenda, and it was no surprise when the DOJ proposed, in mid-June, to amend Section 230 to add "a carve-out for bad actors who … are willfully blind to criminal content on their own services."[9]

This is precisely what the EARN IT Act does. Even though the bill appears to focus only on child sexual exploitation (CSE) content and child sexual abuse material (CSAM),[10] its effect would be much broader: because any website or Internet service that offers private communications *could* be used to transmit CSE/CSAM, the bill would bar them all from using end-to-end encryption, in which only the two parties to a communication hold the encryption keys and the service provider cannot see the communications in unencrypted form. Even though this is the only way to ensure that a communication is truly secure,[11] a plaintiff would be able to allege that the website was "reckless" for engaging in such "willful blindness" (the DOJ's term). Thus, Signal, Facebook's WhatsApp, and Apple's Facetime would have to be re-engineered to be made less secure, and Facebook would have to abandon plans to strong-encrypt its Messenger product. There is no such thing as a backdoor only for the good guys: requiring a backdoor access for U.S. law enforcement and national security agencies exposes users' private communications to attack by foreign governments and malicious hackers.[12]

---

[6] James Comey, Director, Federal Bureau of Investigations, Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course? Address Before the Brookings Institution (Oct. 16, 2014), https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course.

[7] Federal Bureau of Investigations, Going Dark, (last visited June 24, 2020 08:00 PM), *available at* https://www.fbi.gov/services/operational-technology/going-dark.

[8] Press Release, *Department of Justice to Hold a Workshop on Section 230 of the Communications Decency Act*, Department of Justice (Jan. 30, 2020,) https://www.justice.gov/opa/pr/department-justice-hold-workshop-section-230-communications-decency-act.

[9] Press Release, *Justice Department Issues Recommendations for Section 230 Reform*, Department of Justice (June 17, 2020,) https://www.justice.gov/opa/pr/justice-department-issues-recommendations-section-230-reform.

[10] Child Sexual Abuse Material, The National Center for Missing and Exploited Children, (last visited June 24, 2020 08:30 PM,) https://www.missingkids.org/theissues/csam.

[11] *See* Andy Greenberg, *Hacker Lexicon: What is End-to-End Encryption?* WIRED (Nov. 25, 2014, 09:00 AM,) https://www.wired.com/2014/11/hacker-lexicon-end-to-end-encryption/.

[12] Steve Morgan, *Apple's CEO on Encryption You Can't Have a Backdoor that's Only for Good Guys*, FORBES (Nov. 21, 2015, 6:57 AM), https://www.forbes.com/sites/stevemorgan/2015/11/21/apples-ceo-on-encryption-you-cant-have-a-back-door-thats-only-for-the-good-guys/#48684c3f483a.

Under similar theories of recklessness, the EARN IT Act would force ICS providers to make a variety of other changes, including "employing age rating and age gating systems;"[13] age-gating use of encrypted services (so that service providers can monitor their communications), and making it harder for adults and children to communicate with each other.[14] In effect, the bill could revive the Child Online Protection Act of 1998, even though the courts struck down COPA's age verification requirements under the First Amendment.[15] The bill could also be used to force ICS providers to retain user data so that it can be accessed by law enforcement, something proposed in legislation in 2011[16] but that failed after an outcry from privacy advocates across the political spectrum.[17]

The bill coerces companies in three steps: First, the bill creates sweeping new federal civil liability for "recklessly" allowing users to share CSE/CSAM, even in private messages. Second, the bill strips "interactive computer service providers" (ICS providers — Internet sites and services) of their immunity against such liability for user-generated content under Section 230 of the Communications Decency Act of 1996, which currently functions as an immunity not merely from ultimate liability but also from suit.[18] Section 230 allows defendant ICS providers to dispose of lawsuits with a motion to dismiss. Third, the bill allows ICS providers to "earn" back that immunity, either by (a) certifying to compliance with ***all*** of the "best practices" developed by a National Commission on Online Child Sexual Exploitation Prevention, a group convened and dominated by the Attorney General, or (b) proving the reasonableness of their practices. As applied, only the former will allow ICS providers to regain Section 230's shield against litigation because it will be impossible to get a court to grant a motion to dismiss under the "reasonableness" standard. This means a website would

[13] *Id.* at § 4(a)(3)(I).

[14] Riana Pfefferkorn, *The EARN IT Act is Unconstitutional. First Up, the First Amendment*, Ctr. For Internet & Soc'y (Mar. 9, 2020 at 10:53 PM), http://cyberlaw.stanford.edu/blog/2020/03/earn-it-act-unconstitutional-first-first-amendment.

[15] *American Civil Liberties Union v. Mukasey*, 534 F.3d 181 (3d Cir. 2008), *cert. denied*, 555 U.S. 1137 (2009).

[16] Press Release, *Free Market Coalition Opposes Digital Dragnet*, TechFreedom (July 27, 2011) https://techfreedom.org/free-market-coalition-opposes-digital-dragnet/.

[17] *See Id*.

[18] The definition of "interactive computer service provider" plays a key role in the operation of the statute: if a website is "responsible, in whole ***or in part***, for the creation or development of information provided through the Internet or any other interactive computer service," it becomes an "information content provider," not an ICS provider, and thus is not protected by the statute. 47 U.S.C. § 230(f)(3). Thus, for example, Roommates.com was not protected for racially discriminatory housing ads because it solicited racially discriminatory preferences from its users. *Fair v. Roommates,* 521 F.3d 1157, 1169-70 (9th Cir. 2008). By the same token, Backpage.com was not protected by Section 230 for sex trafficking ads it helped to create. *Doe v. Backpages.com, No. 17-11069-LTS*, 2018 U.S. Dist. LEXIS 53198 (D. Mass. 2018) (citing *FTC v. Accusearch, Inc.*, 570 F.3d 1187, 1197 (10th Cir. 2009)).

have to endure broad, expensive and potentially damaging court-ordered discovery by a plaintiff into its internal operations. At best, the affirmative defense of reasonableness could be established later, on a motion for summary judgment, but even this will be difficult because the website would bear the burden of proving its affirmative defense. Consequently, the "Best Practices" will be tantamount to legal mandates.

The drafters intended for this convoluted structure to obscure serious Constitutional problems: the Fourth Amendment's prohibition on unreasonable search and seizures, and the First Amendment's prohibition on the restriction of free speech. Moreover, the structure creates constitutional problems of its own. First, coercing "tech" companies into changing how they design their services—an exercise of editorial discretion protected by the First Amendment—by withholding the protection of Section 230 violates the "unconstitutional conditions" doctrine. Second, the bill violates the Constitution's separation of powers by delegating the drafting of *de facto* regulations to a quasi-governmental body under an intentionally open-ended standard, and then putting a veneer of legislative legitimacy on that document by fast-tracking it through both chambers of Congress but *without* the President's signature, or opportunity for veto. This process violates every tenant of conservative constitutional principal — and yet the bill enjoys the support of leading Republicans and, perhaps, the Department of Justice.

I. How the EARN IT Act Works

A draft version of the EARN IT Act leaked in late January,[19] leading to a wave of criticism focused on a simple narrative: the draft bill gave the Attorney General a procedural backdoor to crack down on encryption online.[20] In response, sponsors of the bill loudly disclaimed any intention to restrict online encryption and made a series of changes to the leaked draft. When sponsors finally introduced the bill on March 5,[21] they claimed they had addressed the

[19] Ben Brody & Naomi Nix, *Lindsey Graham Proposal Could Expose Apple, Facebook to Lawsuits*, BLOOMBERG (Jan. 30, 2020, 2:00 AM), https://www.bloomberg.com/news/articles/2020-01-30/lindsey-graham-proposal-could-expose-apple-facebook-to-lawsuits.

[20] *See, e.g.*, Berin Szóka, *Lindsey Graham's Sneak Attack On Section 230 And Encryption: A Backdoor To A Backdoor?*, TECHDIRT (Jan. 31, 2020, 12:05 PM), https://www.techdirt.com/articles/20200131/11252343832/lindsey-grahams-sneak-attack-section-230-encryption-backdoor-to-backdoor.shtml.; Riana Pfefferkorn, *The EARN IT ACT: How To Ban End-To-End Encryption Without Actually Banning It*, Center for Internet and Society (Jan. 30, 2020, 12:42 PM), https://cyberlaw.stanford.edu/blog/2020/01/earn-it-act-how-ban-end-end-encryption-without-actually-banning-it.

[21] *Graham, Blumenthal, Hawley, Feinstein Introduce EARN IT Act to Encourage Tech Industry to Take Online Child Sexual Exploitation Seriously*, Comm. on the Judiciary (Mar. 5th, 2020) *available at*

concerns raised about the draft. In fact, these changes fail to address the fundamental constitutional problems created by the bill — and raise new ones.

Fully half the bill's text concerns the structure and duties of the Commission (Sections 3 and 4) — with a great deal of material added in the version introduced as legislation. That version added nearly 2500 words.[22] The way the bill is drafted, the way it was amended between the leaked draft and the final version, and the way the bill's sponsors talk about the bill, all serve to focus discussion of the bill on the Commission and the "best practices" it could issue. But these are of distinctly secondary importance. Critically, these "best practices" might *never* go into effect — and yet, even without them, the bill would reshape the Internet.

The bill works first by creating broad new civil and criminal liability for providers of "interactive computer services," and only then offering a provider "safe harbor" immunity from that liability in exchange for either (a) certifying compliance with *all* of the "best practices" developed by the Commission and approved by Congress or (b) taking its chances in court to show that it had "implemented reasonable measures relating to the matters described in section 4(a)(3) …., to prevent the use of the interactive computer service for the exploitation of minors."[23]

Even a careful reader of the bill's text could be forgiven for getting this backwards, because the key provision is buried in the middle of the bill — after a long discussion of the process for drafting best practices and before a laundry list of amendments that would replace every instance of the term "child pornography" with "child sexual abuse material" across the U.S. Code. Furthermore, Section 6 ("Earning Immunity") is so convoluted that it is essentially impossible to understand the effects of this section without carefully parsing both Section 230 *and* 18 U.S.C. § 2255, the provision that currently authorizes civil lawsuits by those exploited for the production of CSAM or CSE. Thus, it is here that one must start in understanding how the EARN IT Act would actually work — and why concerns about the bill cannot be addressed simply by tinkering with the "best practices" process.

---

https://www.judiciary.senate.gov/press/rep/releases/graham-blumenthal-hawley-feinstein-introduce-earn-it-act-to-encourage-tech-industry-to-take-online-child-sexual-exploitation-seriously.

[22] Nearly a third of the text of the bill as introduced includes another addition the leaked draft: replacing references to "child pornography" with "child sexual abuse material" across the U.S. Code. EARN IT Act, S. 3398, 116th Cong., § 7 (2020).

[23] EARN IT Act § 6(a)(B)(ii).

A. Step 1: Expanding Civil Liability Under 2255

CSE and CSAM are governed by two provisions of Title 18: Section 2552 (CSE) and Section 2252A (CSAM). Both work essentially the same way, punishing anyone who distributes, receives, reproduces, promotes, or produces CSE/CSAM.[24] Section 2255, although tucked into the criminal code, provides for recovery of damages through civil suit by "[a]ny person who, while a minor, was a victim of a violation of …" either Section 2252 or 2252A. Historically, suits under Section 2255 have been rare, and generally involve those actually *convicted* under 2252 or 2252A,[25] although a conviction is not an actual prerequisite.[26] Suing third parties involved in the process of distributing CSE/CSAM under 2255 traditionally has been difficult, as the plaintiff must demonstrate actual knowledge of the particular CSE/CSAM, and that the individual depicted in the CSAM is, in fact, a minor.[27] It is on this basis that ICS providers generally have been immune to lawsuits under Section 2255.

The EARN IT Act would fundamentally change this dynamic. For the first time, CSE/CSAM victims would be able to sue websites simply for not doing enough to block 100% of CSE/CSAM material. The EARN IT Act makes this possible by amending (a) amending Section 230 to allow suits under Section 2555 and (b) amending Section 2255 such that a plaintiff need not show "actual knowledge" of the particular CSE/CSAM material, but merely that the ICS provider was "recklessness" in the way it operates generally, a standard that might have nothing to do with CSE/CSAM at all. Such a plaintiff need only show that a "violation" had occurred *but not necessarily that the website was involved*; the criminal conviction of one of the website's user would suffice. Alternatively, a plaintiff might allege that the website itself violated 18 U.S.C. § 2252 or 2252A. While this *would* require proving "actual knowledge" of

---

[24] *See infra* at 15.

[25] *See, e.g., Roe v. City of Waterbury*, 542 F.3d 31 (2d Cir. 2008), judgment entered, 2006 WL 3332978 (D. Conn. Nov. 16, 2006) (plaintiff's Section 2255 suit dismissed because defendant was not "indicted, tried or convicted" of a child sex offense).

[26] *Smith v. Husband*, 376 F.Supp. 2d 603, 607 (E.D. Va. 2005)(the legislative history of Section 2255 "indicates that it was not Congress's intent that a conviction under the other sexual exploitation statutes be a prerequisite to the initiation of a civil suit for damages. The Court finds that legislative history indicates that 18 U.S.C. § 2255 was intended to provide a remedy for victims without requiring a criminal conviction."). A similar civil remedy provision provides that civil actions "shall be stayed during the pendency of any criminal action arising out of the same occurrence in which the claimant is the victim," 18 U.S.C. § 1591(b)(1), making clear that the civil action *could* commence before the criminal action.

[27] *Tilton v. Deslin Hotels, Inc.*, No. 8:05-cv-692-T-30TGW, 2007 WL 3072374 (M.D. Fla. Oct. 19, 2007), *aff'd sub nom. Tilton v. Playboy Entm't Group, Inc.*, 554 F.3d 1371 (11 Cir. 2009) (district court found that "in order to prevail on these claims, plaintiffs must establish that defendants transported, received, distributed, or reproduced for distribution a visual depiction ***knowing, at the time of the transport, receipt, distribution or reproduction,*** that said depiction contained images of a minor engaging in sexually explicit conduct.") (emphasis added).

CSE/CSAM, it would be far easier to prove such a claim under the "preponderance" of the evidence standard of civil litigation than the "beyond a reasonable doubt" criminal standard.

For example, an ICS might be found to be "reckless" in its practices by instituting strong encryption that could allow for sexual predators to distribute CSAM over the ICS without any knowledge of the content of material shared by two parties using encrypted communications. Attorney General Bill Barr laid out the legal case for categorizing the decision to offer strong encryption as "reckless" in a speech last summer:

> Some object that requiring providers to design their products to allow for lawful access is incompatible with some companies' "business models." But what is the business objective of the company? Is it "A" — to sell encryption that provides the best protection against unauthorized intrusion by bad actors? Or is it "B" — to sell encryption that assures that law enforcement will not be able to gain lawful access? I hope we can all agree that if the aim is explicitly "B" — that is, if the purpose is to block lawful access by law enforcement, whether or not this is necessary to achieve the best protection against bad actors — then such a business model, from society's standpoint, is illegitimate, and so is any demand for that product. The product jeopardizes the public's safety, with no countervailing utility. ...
>
> The real question is whether the residual risk of vulnerability resulting from incorporating a lawful access mechanism is materially greater than those already in the unmodified product. The Department does not believe this can be demonstrated.[28]

This same theory could be used by CSE/CSAM victims to sue ICS providers for being "reckless" in making other design decisions, such as not retaining user data, not age-gating users, not segmenting user by age, *etc*. The bill also includes, as a category of recommendations, "offering parental control products that enable customers to limit the types of internet websites and content accessible to children" — a broad category that allow the Commission to develop best practices that no connection with CSAM/CSE at all.[29]

---

[28] *Attorney General William P. Barr Delivers Keynote Address at the International Conference on Cyber Security*, U.S. Dept. of Justice (July 23, 2019), https://www.justice.gov/opa/speech/attorney-general-william-p-barr-delivers-keynote-address-international-conference-cyber.

[29] EARN IT Act § 4(a)(3)(1)(J). The "Christmas tree" effect of this provision could allow the Commission to define all manner of "best practices," including related to advertising practices that have profound First Amendment implications.

B. Step 2: Transforming Litigation by Amending Section 230.

As discussed above, civil actions against ICS providers (and others in the distribution chain of CSE/CSAM) under Section 2255 currently require "actual knowledge" that the material was CSE/CSAM (including demonstrating knowledge that the persons depicted in CSAM, or victims of CSE, were minors). As a result, plaintiffs carry a heavy burden, and cases have rarely been brought against ICS providers — even by plaintiff's lawyers who view "big tech" companies as having "deep pockets" and as willing to settle early to avoid the costs of litigation (both financial and reputational).

The EARN IT Act lowers the plaintiff's burden, requiring only that it show, by a preponderance of the evidence (the standard for civil litigation) that an ICS provider was "reckless" in its practices. For the first time, a plaintiff will be able to bring a 2255 civil action against a party that has not been convicted of a criminal violation, which requires not only actual knowledge but also that the government prove its case "beyond a reasonable doubt."

Most importantly, because "recklessness" is such a vague standard, an ICS provider could never hope to get out from under a Section 2255 lawsuit at the motion to dismiss, or even summary judgment, stage. Plaintiffs would subject ICS providers to massive discovery requests, where the bulk of litigation costs reside,[30] subjecting defendants to the "death by ten thousand duck-bites" warned about in *Roommates.*[31] Dueling experts would tee off on whether each and every practice and design decision of an ICS provider was "reckless" or "reasonable," both subjective terms that are inherently fact-driven, providing no "early out" for a defendant from oppressive litigation.

C. Step 3: Regaining Section 230 Immunity

The only practical way out of being dragged into endless litigation will be for ICS providers to certify to compliance with ***all*** of the "Best Practices" developed by the Commission and approved by both chambers of Congress (but *not*, unlike normal legislation, signed by the President or subject to veto). In practice, this means agreeing to whatever demands the

[30] "The costs of litigation, as we all know, have become staggering. A plaintiff may put a defendant or a defendant may put a plaintiff to a tremendous amount of expense . . . in defending or prosecuting a case." *Crawford Fitting Co. v. J.T. Gibbons, Inc.,* 482 U.S. 437, 450 (1987). The bulk of that expense—sometimes up to 90 percent— arises out of discovery. See Memorandum from Paul V. Niemeyer, Chair, Advisory Committee on Civil Rules, to Hon. Anthony J. Scirica, Chair, Committee on Rules of Practice and Procedure (May 11, 1999), 192 F.R.D. 354, 357 (2000).

[31] *Roommates,* 521 F.3d at 1174 (9th Cir. 2008) ("section 230 must be interpreted to protect websites not merely from ultimate liability, but from having to fight costly and protracted legal battles.").

government (acting through the cat's paw of the Commission) makes in order to qualify as "reasonable," and not "reckless," even if those demands are constitutionally suspect.

Crucially, the bill's amendments to Section 230 and 2255 will go into effect either one year after a "Best Practices" resolution is approved by Congress or within four years of enactment of the EARN IT Act.[32] This means companies will face new liability whether or not any Best Practices are ever finalized. Given the ineffectiveness of the "Reasonableness" affirmative defense, tech companies will have a very strong incentive to push for the Commission to issue its "Best Practices," and for the Attorney General and Congress to approve them, as quickly as possible. This places extraordinary power in the hands of the Attorney General, who will chair and dominate the Commission, to specify "best practices" that further the government's agenda, with little to nothing to do with protecting children from predation.

Once the Best Practices have been approved by Congress, any website that chooses *not* to certify to compliance with *all* of them, and instead tries establish the reasonableness of its practices, will face an even more daunting task: divergences between a company's practices and the Commission's recommendations may be treated as presumptively unreasonable.

D. Development and Issuance of Best Practices

The bill establishes a National Commission on Online Child Sexual Exploitation Prevention, composed of 19 members: the Attorney General, Secretary of Homeland Security, and FTC Chairman (or their proxies) plus 16 members chosen by House and Senate leaders (four for each party's leaders in each chamber). Each member shall serve a five-year term and will be replaced as necessary under the same requirements so that the Commission is effectively permanent. "Not less frequently than once every 5 years, the Commission shall update and resubmit to the Attorney General recommended best practices…."[33]

The Commission would hold its first meeting no later than "60 days after the date on which a majority of the members of the Commission have been appointed." The Attorney General would chair the Commission, and convene it at will. No less than 18 months after a majority of the members have been appointed, the Commission must develop and submit to the Attorney General recommended best practices for providers of interactive computer services. To recommend the best practices, a supermajority (14/19 = 74%), must support them. This may seem to guard against abuse, but in practice, the Commission will likely be heavily stacked against the tech industry. Counting the members from the FTC, DOJ, and

[32] EARN IT Act § 6(c).

[33] EARN IT Act § 4(a)(5).

Department of Homeland Security, plus two from law enforcement, two prosecutors, and two who either work with victims or are survivors of online child sexual exploitation, the Commission would include nine reliable votes for "getting tough."[34]

Moreover, as explained above, tech companies will be so dependent upon the finalization of best practices in order to regain Section 230 immunity that even those on the Commission sympathetic to industry or privacy concerns will have a strong incentive to vote to approve Best Practices — no matter how strongly they may object to their substance.

The Attorney General must "approve or deny" the recommended best practices within 30 days. A denial must be explained in public written findings. If approved, the best practices must be published on the website of the Department of Justice and in the Federal Register. The Attorney General must also submit the recommended best practices to Congress, including the Committee on the Judiciary and the Committee on Commerce, Science, and Transportation of the Senate, and the Committee on the Judiciary and the Committee on Energy and Commerce of the House of Representatives.

On the day the Attorney General submits the recommended best practices to Congress, leadership in the Senate and the House of Representatives will introduce a resolution[35] containing only the recommended best practices in their entirety. The Act "fast tracks" the recommended best practices in three ways: (1) if the Congressional committees assigned (by House and Senate leadership) fail to report the resolution to the House or Senate no later than 45 days after the date of introduction, the resolution will automatically be sent to the floor of each chamber; (2) no amendments will be allowed on the floor, the time for debate will be very short, and the normal procedural motions used to tie up legislation (especially in the Senate) will be unavailable; and (3) the covered bill will go into effect *without* signature by the President (or the opportunity for veto).

II. Government as "Encourager": the EARN IT Act Attempts to Circumvent the Fourth Amendment's Warrant Requirement.

The EARN IT Act avoids directly requiring any changes in how ICS providers operate, lest doing so subject them to the Fourth Amendment's requirement that a judge authorize searches and seizures of private communications by assessing whether a showing of probable cause has been made that would justify violating "[t]he right of the people to be

[34] *See* Szóka, *supra* note 20.

[35] Technically, the EARN IT Act refers to this as a "covered bill," but it is referred to herein as a "resolution" to avoid confusion with "the bill" (used to refer to the EARN IT Act).

secure in their [communications] the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, against unreasonable searches and seizures."[36] This risks undermining both CSE/CSAM convictions and the system of voluntary cooperation between ICS providers and law enforcement to stop CSE/CSAM.

A. Section 230 Hasn't Prevented the Fight Against CSE/CSAM

The existing system for policing CSAM online was carefully designed to maximize both self-policing of CSAM by tech companies and their cooperation with law enforcement in ensuring the prosecution of those who generate, distribute and view it. Section 230 has never protected tech companies from prosecution under federal criminal law,[37] but the law does protect them from civil liability (and prosecution under state criminal laws).[38]

Some child protection advocates are frustrated with the status quo. Last summer, the National Center for Missing and Exploited Children (NCMEC) raised three specific objections (besides woeful under-funding of CSAM enforcement):

1. While 18 U.S.C. § 2258A requires ICS providers to make reports to NCMEC whenever they have "actual knowledge" of violations of six criminal statutes involving CSAM or CSE, the "the facts and circumstances included in each report" are left up to the "sole discretion of the provider."[39] Thus, the nature of reporting to NCMEC varies significantly by company.
2. Most significantly, many ICS providers report CSAM/CSE incidents on their services but do not "provide the actual images or videos they are reporting."[40]

---

[36] U.S. Const. amend. IV.

[37] 47 U.S.C. § 230(e)(1).

[38] 47 U.S.C. § 230(c)(1). *See Zeran v. America Online*, 129 F.3d 327, 330 (4th Cir. 1997) (", Section(s) 230 precludes courts from entertaining claims that would place a computer service provider in a publisher's role. Thus, lawsuits seeking to hold a service provider liable for its exercise of a publisher's traditional editorial functions — such as deciding whether to publish, withdraw, postpone or alter content — are barred."). 47 U.S.C. § 230(e)(1) excludes federal, but not state, criminal law.

[39] 18 U.S.C. § 2258A(b).

[40] *Protecting Innocence in a Digital World: Before the S. Comm. on the Judiciary*, 116th Cong. 2 (2019) (statement of John F. Clark, President, National Center for Missing & Exploited Children), https://www.judiciary.senate.gov/download/clark-testimony&download=1.

3. ICS providers should report not only CSAM, but also "types of child sexual exploitation that are not specifically enumerated within the federal statute, such as child sex trafficking, but which are common forms of online child sexual exploitation."[41]

These are all reasonable concerns which Congress has long had the opportunity to address with direct mandates. One must ask *why* Congress has not done so. NCMEC also complained that that some ICS providers do not "proactively search or screen their networks for [CSAM]"[42] — another formulation of DOJ's complaint about "willful blindness." Yet, as recently as late 2018, Congress updated ICS providers' reporting duties under 18 U.S.C. § 2258A, but chose *not* to impose the kind of filtering mandate that NCMEC wants.[43] The statute continues to require providers to report only CSAM they "obtain[] actual knowledge of."[44] Ultimately, Congress has not imposed mandatory filtering because of Fourth Amendment doctrine holding that the Constitution's warrant requirement applies not only to law enforcement agencies but also private actors operating under governmental coercion.[45]

B. Direct Mandates to Collect Evidence Risk Converting Internet Sites & Services into Government Actors.

Directly requiring ICS providers to collect evidence of violations of criminal law could lead a court to decide that ICS providers are "government actors" subject to the Fourth Amendment,[46] just as the Tenth Circuit has ruled that NCMEC, nominally a private non-profit, is a government actor.[47] This, in turn, would mean that courts would have to issue a warrant, based on a finding of probable cause to believe a crime had been committed, before ICS providers could perform "searches" of private communications and turn over evidence to

---

[41] *Id*.

[42] *Id*.

[43] CyberTipline Modernization Act of 2018, Pub. L. No. 115–395, 132 Stat. 5287, available at https://www.govinfo.gov/content/pkg/PLAW-115publ395/pdf/PLAW-115publ395.pdf.

[44] EARN IT Act § 9.

[45] Prior to 2010, the government argued that private communications such as emails stored by intermediaries were not protected by the Fourth Amendment because of the "third party doctrine," but the Sixth Circuit clearly rejected these arguments in *Warshak v. United States*, ruling that "individuals maintain a reasonable expectation of privacy in e-mails that are stored with, or sent or received through, a commercial ISP." *Warshak v. United States*, 631 F.3d 266, 288 (6th Cir. 2010).

[46] *See generally* Alexandra L. Mitter, *Deputizing Internet Service Providers: How the Government Avoids Fourth Amendment Protections*, 67 NYU Ann. Surv. Am. L. 235 (2011), https://www.law.nyu.edu/sites/default/files/upload_documents/NYU-Annual-Survey-67-2-Mitter.pdf.

[47] *United States v. Ackerman*, 831 F.3d 1292 (10th Cir. 2016).

NCMEC or other government actors.[48] In short, direct mandates could bring the entire system of cooperation between ICS providers and law enforcement crashing down. Individuals convicted of creating, distributing, or viewing CSAM/CSE under 18 U.S.C. §§ 2252 & 2252A could have their convictions invalidated if the evidence used against them was collected via a "voluntary" reporting to NCMEC.[49]

Given this constitutional backdrop, we understand why lawmakers are trying to find a round-about way to change how tech companies handle CSAM. Nonetheless, the approach taken by EARN IT creates enormous risks for law enforcement and remains unnecessarily overbroad in the effects that it would have for law-abiding Americans.

Again, conditioning Section 230 immunity against (significantly increased) Section 2255 liability on compliance with "best practices" developed by a commission operating under the supervision and, effectively, direction of the Attorney General, may be tantamount to issuing direct mandates — which may convert nominally private actors into government actors for Fourth Amendment purposes.[50] "A private search will be subject to Fourth Amendment restrictions where the conduct has 'as its purpose the intention to elicit a benefit for the government in either its investigative or administrative capacities.'"[51] The benefit to the government is obvious: assisting in the prosecution of CSAM/CSE laws. Furthermore, since the underlying purpose of the EARN IT Act is to change the practices of ICS providers (to "best" practices), it would be difficult to argue that an ICS provider that changes its practices does so "to serve its own ends." If the government acts "directly as a participant . . . or indirectly as an encourager," then a private actor likely intends to assist law enforcement and is thus "an instrument of the government."[52] Using Section 230 as the mechanism of "encouragement" may be considered tantamount to a reward.[53] As Justice Gorsuch, then a Tenth Circuit judge, explained in *Ackerman*, circuit courts have varied in the tests they have applied to determine whether an entity is a government actor.[54] The First Circuit has considered "[1] the extent of the government's role in instigating or participating in the

[48] Mitter, *supra* note 46.

[49] *See, e.g., Wong Sun v. United States*, 371 U.S. 471, 484-85, 488 (1963); *Silverthorne Lumber Co., v. United States*, 251 U.S. 385, 391-92 (1920).

[50] *Ackerman*, 831 F.3d 1292.

[51] *United States v. Attson*, 900 F.2d 1427, 1431 (9th Cir. 1990); Mitter, *supra* note 46.

[52] *United States v. Leffall*, 82 F.3d 343, 347 (10th Cir. 1996) ("A government agent must be involved either directly as a participant—not merely as a witness--or indirectly as an encourager of the private person's search before we will deem the person to be an instrument of the government.").

[53] Mitter, *supra* note 46, at 217 (citing *United States v. Ginglen*, 467 F.3d 1071, 1074 (7th Cir. 2006), *United States v. Shahid*, 117 F.3d 322, 325 (7th Cir. 1997)).

[54] 831 F.3d at 1301.

search, [2] its 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."[55] The Tenth Circuit has asked "1) whether the government knew of and acquiesced in the intrusive conduct, and 2) whether the party performing the search intended to assist law enforcement efforts or to further his own ends."[56]

Under either test, the EARN IT Act could lead a court to rule that ICS providers are performing "searches" of CSAM and CSE material subject to the Fourth Amendment as government actors.

As noted above, the fact that the bill appears to offer an alternative — ICS providers which chose not to certify compliance with *all* of the Commission's recommendations may regain Section 230 protections by establishing the "reasonableness" of their practices[57] — will likely be of little use to companies facing the risk of multiple lawsuits filed under 18 U.S.C. § 2255. While the drafters of the EARN IT Act doubtless added this provision in order to bolster arguments that the bill does not convert ICS providers into government actors, it may make little difference to a court's analysis, especially if few ICS providers chose not to certify compliance with the Commission's "best practices." Justice Gorsuch's commentary in *Ackerman* bears emphasis:

> [S]ince time out of mind the law has prevented agents from exercising powers their principals do not possess and so cannot delegate. That is a rule of law the founders knew, understood, and undoubtedly relied upon when they drafted the Fourth Amendment—for what would have been the point of the Amendment if the government could have instantly rendered it a dead letter by the simple expedient of delegating to agents investigative work it was forbidden from undertaking itself? Indeed, it's long since accepted that the Amendment's proscriptions apply not just to governmental entities but also to those who serve as the government's agents in particular cases.[58]

Regardless of how a court actually rules on these Fourth Amendment questions, it would likely take at least three years for an initial decision, and probably longer. Prosecutors attempting to bring to justice those who have heinously exploited children, or distributed recordings of their abuse, will face a constant barrage of Fourth Amendment arguments

---

[55] *See, e.g., United States v. Silva*, 554 F.3d 13, 18 (1st Cir. 2009).

[56] *United States v. Souza*, 223 F.3d 1197, 1201 (10th Cir. 2000).

[57] EARN IT Act § 6(a)(6)(B)(ii).

[58] 831 F.3d at 1300 (internal citations omitted) (citing numerous attempts by the government to cloak a government entity as a private party).

raised by every criminal defendant whose communications were "searched" *after* the Commission's "best practices" had gone into effect (the bill gives the Commission 18 months[59]). And after a district court rules on this evidence, the case will have to work its way through the appeals process, leaving countless other cases, and convictions, in limbo, especially if courts in different judicial circuits reach different conclusions as to the Fourth Amendment implications of the EARN IT Act.

In short, the EARN IT Act contains a ticking constitutional time bomb that could take years to go off. If a court finds that the bill converts tech companies into government actors, compelling them to collect CSAM evidence, such a decision could jeopardize *all* convictions of those directly generating, trafficking and consuming CSAM. Yes, Congress could then go back to the drawing board, but these individuals would go unpunished — and there would be a period of chaos, during which ICS providers may simply cease cooperating with law enforcement. Even before such a decision, the risk that it could happen will only discourage law enforcement from investing their limited resources in enforcing existing federal law.

III. The EARN IT Act Violates the First Amendment.

The EARN IT Act violates the First Amendment for much the same reason the courts have blocked previous congressional efforts to "clean up the Internet": they burden not only obscenity but also lawful speech by users, as well as the rights of ICS providers to design their services as they see fit. The fundamental problem is not the "best practices" contemplated by the bill, though their breadth does help to illustrate the potential effects of the bill, but the recklessness standard at the heart of the bill. That standard is unconstitutionally vague and would have sweeping effects on lawful speech.

A. The EARN IT Act Will Fail Strict Scrutiny.

The EARN IT Act may *appear* not to implicate the First Amendment because the new civil liability it creates is only for CSE/CSAM and the Supreme Court has "long held that obscene speech—sexually explicit material that violates fundamental notions of decency—is not protected by the First Amendment."[60] The Court upheld a state law banning "obscene material depicting (actual or virtual) children engaged in sexually explicit

[59] EARN IT Act § 4(a)(1)(A).

[60] *See United States v. Williams*, 553 U.S. 285, 288 (2008).

conduct, and any other material depicting actual children engaged in sexually explicit conduct."[61] Thus, Sections 2252, 2252A, and 2255 have never been successfully challenged.

But the EARN IT Act will affect far more than just CSE/CSAM; indeed, the list of "matters" to be addressed by "Best Practices" makes clear that the purpose of the bill is to force ICS providers to make fundamental changes to the design of their service that will affect broad swathes of lawful speech. Consider one such matter: "preventing, identifying, disrupting, and reporting child sexual exploitation."[62] Using strong encryption means giving up the ability to monitor user communications — including for CSE/CSAM. "Government efforts to control encryption thus may well implicate not only the First Amendment rights of cryptographers intent on pushing the boundaries of their science, but also the constitutional rights of each of us as potential recipients of encryption's bounty."[63] By the same token, an ICS provider may feel compelled to filter or retain user communications. Another "matter" is "employing age rating and age gating systems to reduce child sexual exploitation."[64] These sweeping impacts on lawful speech make the EARN IT Act unconstitutional for the same reasons as the Communications Decency Act:

> According to the Government, the CDA is constitutional because it constitutes a sort of "cyberzoning" on the Internet. But the CDA applies broadly to the entire universe of cyberspace. And the purpose of the CDA is to protect children from the primary effects of "indecent" and "patently offensive" speech, rather than any "secondary" effect of such speech. Thus, the CDA is a content-based blanket restriction on speech, and, as such, cannot be "properly analyzed as a form of time, place, and manner regulation."[65]

As the Supreme Court further explained in *Reno v. ACLU* (1997), the CDA necessarily burdened the lawful speech of adults:

> Given the size of the potential audience for most messages, in the absence of a viable age verification process, the sender must be charged with knowing that one or more minors will likely view it. Knowledge that, for instance, one or more members of a 100-person chat group will be a minor — and therefore that it

[61] 553 U.S. at 293.

[62] EARN IT Act § 4(a)(3).

[63] *Bernstein v. United States Dept. of Justice*, 176 F.3d 1132, 1146 (9th Cir. 1999).

[64] *Id*. § 4(a)(3).

[65] *Reno v. American Civil Liberties Union*, 521 U.S. 844, 867-68 (1997).

> would be a crime to send the group an indecent message — would surely burden communication among adults.[66]

An appellate court later struck down COPA because of much the same overbreadth. The law held websites criminally liable for allowing minors to access "indecent" content that was not necessarily obscene, but that might be harmful to children, such as pornography involving adults — but recognized an affirmative defense: restricting access to such content by *all* users through age verification. This violated the speech rights of adults: "many users who are not willing to access information non-anonymously will be deterred from accessing the desired information."[67] The provision of a credit card remains the standard means used for age verification; thus, the problem of deterring lawful speech by adults remains unchanged.

EARN IT creates (a) similarly broad liability for allowing harmful activity to take place, and an (b) an affirmative defense that serves as a *de facto* mandate. But where COPA's affirmative defense was simple and clear (age-gating access) and directly related to the source of liability (allowing minors to access indecent content), EARN IT effectively forces ICS providers to sign onto a broad set of requirements that may be only vaguely related to the source of liability and will only be determined later. This makes EARN IT far *more* constitutionally problematic than COPA: where COPA affected only the right of adults to access potentially "indecent" material anonymously, EARN IT will affect the entire experience of using certain Internet services for all users, irrespective of the nature of their content.

The bill's reference to using "age gating systems to reduce child sexual exploitation" suggests the "best practices" may require ICS providers to segment users by age, which seriously infringes on the First Amendment rights of adults to communicate. As Riana Pfefferkorn, Associate Director of Surveillance and Cybersecurity at the Stanford Center for Internet and Society explains:

> *Scenario 1: Facebook.* The teenage boy is the only child of a single mother who has no other living family except her brother. The mom isn't on Facebook, but her son is. The adult man is her brother, who joins Facebook and wants to friend his nephew and use Facebook Messenger to chat with him. The two accounts have no friends in common, the users have different last names, and they live in two far-apart cities, so to Facebook it looks like they don't even know each other. Given all of those data points, in order to avoid the risk of liability under EARN IT,

[66] *Id*. at 876.

[67] *Mukasey*, 534 F.3d at 196 (citing *American Civil Liberties Union v. Gonzales*, 478 F. Supp. 2d 775, 806 (E.D. Pa. 2007)).

> Facebook bars the uncle from being able to even friend his nephew at all, much less chat with him.
>
> *Scenario 2: Twitter.* The adult man is a urologist who's become an unlikely celebrity on Twitter due to his open, frank, and cheerful approach to discussing sexual health. He leaves his DMs open so that any user can message him privately, even if he doesn't follow that user. The teenage boy has some questions which he's too embarrassed to ask his pediatrician, so he DMs the urologist, using slang language for body parts and sex acts. The urologist DMs back, in a professional tone, using appropriate medical terminology, and answers his questions. Twitter DMs are not end-to-end encrypted (yet), so Twitter can "see" their content. Due to EARN IT, the company has begun scanning all DMs for potential grooming/enticement (something it already does for certain other purposes). It detects that a minor's account has contacted an adult's account, the latter replied back, they don't follow each other or have followers in common, and the DMs they've exchanged contain sexual words. Twitter flags the DMs for review by an internal team and suspends the urologist's account pending the outcome of the review. Twitter also notifies the urologist that his account is being investigated and, depending on the result, his account may be terminated and he will be banned from the service permanently, in accordance with a "one strike" rule instituted in order to avoid liability under EARN IT.
>
> These are just two simple examples of how the EARN IT Act would result in the unconstitutional censorship of perfectly legal speech. Adults and children have a First Amendment right to talk to each other, even when that speech takes place online. Minors have a First Amendment right to seek and receive information about their health, including their sexual health. Yet in the name of cutting down on grooming or enticement online, the EARN IT Act would result in the censorship of vast amounts of constitutionally protected speech.[68]

There is an important but subtle detail here: while both Sections 2252 and 2252A both focus on the "visual depiction … of a minor engaging in sexually explicit conduct,"[69] Section 2252A also bars the "solicitation" and "promotion" of such imagery that may be used for the grooming or enticement of minors. This means, as Pfefferkorn explains, that:

> Enticement and grooming behavior can involve CSAM (e.g. showing a child sex abuse image to a potential child victim in order to normalize abuse). But it also involves, basically, free-text conversations between two individuals. That is: it involves online speech, which, in general, is protected by the First Amendment

[68] Pfefferkorn, *supra* note 14.

[69] 18 U.S.C. §§ 2252(a)(1)(A) & 2252A(a)(3)(B).

> just like offline speech. There are many kinds of illegal online content, some more clear-cut than others. The further away you get from CSAM—the most open-and-shut, clearly-illegal kind of illegal online content in existence (and even then it's not crystal clear)—the harder it becomes to spot the unlawful content. That's especially true at the huge-scale volume of content on popular online services.[70]

This scale problem lies at the heart of the *Reno* decision.[71] Pfefferkorn adds another complication: "it's more difficult than you might think even to figure out which images are in fact unlawful CSAM that falls outside the First Amendment. Restricting EARN IT only to CSAM would *still* implicate the First Amendment in light of the potential for providers to censor protected speech, because line-drawing, even with imagery, isn't easy."[72] In 2002, the Supreme Court held that even virtual depictions of minors engaged in sex acts are fully protected speech.[73]

Pfefferkorn continues, noting that: "[e]ven cartoons [and other artworks], which are protected by the First Amendment, get reported to NCMEC as CSAM, meaning they'd be at risk of censorship under EARN IT best practices."[74]

In short, the EARN IT Act is *designed* to affect user speech that is not CSE/CSAM. "The principal inquiry in determining content neutrality . . . is whether the government has adopted a regulation of speech because of disagreement with the message it conveys."[75] Because the law clearly targets some *lawful* speech, it is a content-based restriction and thus subject to strict scrutiny,[76] which it is highly unlikely to survive. Suppressing the spread of CSE/CSAM may be a highly compelling government interest (the first prong), but the law is clearly not "narrowly tailored" to that purpose (the second prong). This is what the *Mukasey* court said of COPA,[77] but at least COPA's age verification mandate was clear; the EARN IT Act's amorphous approach to the problem is necessarily even less narrowly tailored."

---

[70] *See* Pfefferkorn, *supra* note 14.

[71] *See Reno,* 521 U.S. at 876; *supra* note 66 and associated text.

[72] *See Id*.

[73] *Ashcroft v. Free Speech Coalition*, 535 U.S. 234 (2002).

[74] *Id*. *See* Letter from Prostasia Foundation, National Coalition Against Censorship, Article 19, and the Comic Book Legal Defense Fund to Denton Howard, Executive Director of INHOPE (Jan. 20, 2020) https://prostasia.org/wp-content/uploads/2020/01/Letter-to-Internet-hotlines.pdf ("artistic images should not be added to image hash lists that INHOPE members maintain, and should not be reported to authorities, unless required by the law where the hotline operates.").

[75] *Ward v. Rock Against Racism*, 491 U.S. 781 (1989).

[76] *R.A.V. v. City of St. Paul*, 505 U.S. 377, 382 (1992).

[77] *Mukasey*, 534 F.3d at 188.

The EARN IT Act would also fail the final prong of strict scrutiny: "A statute that 'effectively suppresses a large amount of speech that adults have a constitutional right to receive and to address to one another . . . is unacceptable if less restrictive alternatives would be at least as effective in achieving the legitimate purpose that the statute was enacted to serve."[78] "[T]he burden is on the Government to prove that the proposed alternatives will not be as effective as the challenged statute."[79] The Government's burden is "not merely to show that a proposed less restrictive alternative has some flaws; its burden is to show that it is less effective."[80] Here, the government could use a variety of less restrictive means to address CSE/CSAM, starting with increasing funding for enforcement,[81] deputizing state and local prosecutors to assist in enforcing federal law,[82] and subsidizing the use of CSE/CSAM reporting or filtering tools by companies.

B. The Recklessness Standard Is Substantially Overbroad and Void for Vagueness.

A law burdening speech will be struck down as invalid on its face for "overbreadth" if the government's interest insufficiently "substantial," "judged in relation to the statute's plainly legitimate sweep."[83] In *Reno*, the Supreme Court struck down most of the CDA's prohibition on "indecent" or "patently offensive" speech if accessible to minors: " In order to deny minors access to potentially harmful speech, the CDA effectively suppresses a large amount of speech that adults have a constitutional right to receive and to address to one another."[84]

Likewise, under the Due Process clause of the Fifth Amendment, "laws so vague that a person of common understanding cannot know what is forbidden are unconstitutional on their face."[85] Where such a law implicates the First Amendment, courts may strike down the law as facially unconstitutional.[86] The *Reno* Court analyzed the vagueness of the CDA "because of

---

[78] *Id*. at 198 (quoting *Ashcroft v. American Civil Liberties Union*, 542 U.S. 656, 665 (2004)).

[79] *Ashcroft*, 542 at 665.

[80] *Id*. at 669.

[81] *See infra* notes 143 & 144 and associated text.

[82] 28 U.S.C. § 543(a) ("The Attorney General may appoint attorneys to assist United States attorneys when the public interest so requires").

[83] *Riley v. Nat'l Fed'n of the Blind of N.C., Inc*., 487 U.S. 781, 798 (1988); *Broadrick v. Oklahoma*, 413 U.S. 601, 615 (1973).

[84] *Reno*, 521 U.S. at 874.

[85] *Coates v. City of Cincinnati*, 402 U.S. 611, 616 (1971) (Black, J. concurring).

[86] *Id*. at 619.

its relevance to the First Amendment overbreadth inquiry," but ultimately found it unnecessary to resolve the vagueness challenge to the law under the Fifth Amendment.[87]

The EARN IT Act both significantly more overbroad and significantly vaguer than the CDA. The "sweep" of current CSE/CSAM law is clear: both criminal liability (under Sections 2252 or 2252A) and civil liability (under Section 2255) attach only with actual knowledge of CSE/CSAM. But it is impossible to say what conduct may give rise to civil liability under the EARN IT Act's new "recklessness" standard — and thus to determine the true "sweep of the EARN IT Act. The "matters addressed" by the Commission are textbook examples of overbreadth and vagueness:

- "preventing, identifying, disrupting, and reporting child sexual exploitation"
- "retaining child sexual exploitation content and related user identification and location data"
- "employing age rating and age gating systems to reduce child sexual exploitation" —
- "offering parental control products that enable customers to limit the types of websites, social media platforms, and internet content that are accessible to children;"

These "matters" would be vastly overbroad if they were the subject of direct mandates. The fact that the EARN IT Act approaches these indirectly through the recklessness standard of new civil liability under Section 2255 only magnifies the overbreadth and vagueness of the law. That standard is designed to have the broadest possible effect in reshaping the design of Internet services — and, indeed, it would do so even *without* the issuance of "best practices" or their final approval by both chambers of Congress.

Attorney General Barr's speech last year provides some sense of how courts might apply the EARN IT's "recklessness" standard: again, "[t]he real question is whether the residual risk of vulnerability resulting from incorporating a lawful access mechanism is materially greater than those [security risks] already in the unmodified product."[88] Barr discounts the value of strong encryption by failing even to acknowledge its privacy benefits or the way it enables speech, but he does at least implicitly recognize some weighing test here: "materially" must be measured against *something* — he just does not say what that something would be.

By drawing an analogy to product design more generally, Barr implies that the EARN IT Act's recklessness standard might be guided by tort law. The Third Restatement of Torts provides:

---

[87] *Reno*, 521 U.S. at 864.

[88] FBI Going Dark, *Supra* note 7; Barr, *Supra* note 28.

> **§2. Recklessness**. A person acts recklessly in engaging in conduct if: (a) the person knows of the risk of harm created by the conduct or knows facts that make the risk obvious to another in the person's situation, and (b) the precaution that would eliminate or reduce ***the risk involves burdens that are so slight relative to the magnitude of the risk as to render the person's failure to adopt the precaution a demonstration of the person's indifference to risk***.[89]

This definition replaces Second Restatement of Torts' definition, which has been called "virtually incomprehensible."[90]

> **§500. Reckless Disregard of Safety Defined**. The actor's conduct is in reckless disregard of the safety of another if he does an act or intentionally fails to do an act which it is his duty to the other to do, knowing or having reason to know of facts which would lead a reasonable man to realize, not only that his conduct creates an unreasonable risk of physical harm to another, but also that ***such risk is substantially greater than that which is necessary to make his conduct negligent***.[91]

The Third Restatement has yet to be finalized, meaning that the tort law of recklessness remains in a state of confusion. But under either definition, it remains unclear what, exactly, is to be weighed against risks to others (here, the risk of CSAM/CSE trafficking). In general, though, the answer is, essentially, economic cost: in tort, recklessness liability punishes companies that could avoid a known harm to others by making an additional investment in their product that is "slight" relative to the risk.

But the true "costs" that would be imposed by the EARN IT Act are not the financial costs of engineering "safer" systems. Indeed, tech companies spend *more* money to build end-to-end encryption into their services,[92] but do so because they believe the (a) benefits of strong encryption to users in security and willingness to speak freely, without fear of their communications being compromised, exceed both (b) the economic costs of offering it *and* (c) the societal "costs" of not being able to access those users' private communications, even

---

[89] Restatement of Torts, 3rd, §2. In the criminal context, "the Supreme Court has ... explained that the criminal law generally permits a finding of recklessness only when persons disregard a risk of harm of which they are aware. *See Farmer v. Brennan*, 511 U.S. 825, 836-37 (1994).

[90] Geoffrey Christopher Rapp, *Torts 2.0: The Restatement 3rd and the Architecture of Participation in American Tort Law*, https://open.mitchellhamline.edu/cgi/viewcontent.cgi?article=1409&context=wmlr

[91] Restatement of Torts, 2nd, §500 (1977).

[92] Fortune 1000 companies spend around $2.4 billion per year on custom cybersecurity, including encryption, to safeguard their information but also to mitigate the high costs associated with an eventual data breach. *See* Christopher Hooton, *The Rising Importance of Strong Encryption For U.S. Interests*, Internet Association (June 15, 2017), https://internetassociation.org/publications/rising-importance-strong-encryption-u-s-interests/.

when asked to do so by law enforcement. Companies might save money by deciding not to age-verify or age-segment their users, or retain user data for longer periods, but these decisions have an even more direct impact on the speech interests of users than does the decision to use strong encryption.

The Supreme Court *has* applied a recklessness standard to speech in one area: defamation law. Most notably in *New York Times Co. v. Sullivan* (1964), the Court barred a "public official from recovering damages for a defamatory falsehood relating to his official conduct unless he proves that the statement was made with 'actual malice' — that is, with knowledge that it was false or with ***reckless disregard*** of whether it was false or not."[93] But note just how different this is from the EARN IT Act: here, recklessness is measured with respect to the truth or falsity of a claim — an objectively verifiable question. By contrast, the EARN IT Act's recklessness standard asks an inherently *subjective* question about the weighing of the interests of law enforcement against the speech interests of users (and the economic and other interests of service providers). Such a question might be appropriate for Congress to decide by creating specific requirements, but it cannot simply be left to the courts to apply. Doing so denies ICS providers the clarity of law guaranteed to them by the Fifth Amendment and, as we have seen, the resulting vagueness creates overly broad impacts upon speech that the First Amendment forbids. At a minimum, there is no way civil actions predicated upon such an unclear standard could be resolved at a motion to dismiss, and probably not even at a motion for summary judgment; the fact that such actions would likely have to be resolved at trial greatly increases the *in terrorem* effects of the recklessness standard on how websites design their services.[94]

EARN IT may seem less constitutionally problematic than COPA in one respect: COPA imposed criminal liability, while EARN IT merely creates *civil* liability. But in *Sullivan*, the Supreme Court made clear that this not change the First Amendment analysis, which focuses on how government action affects speech:

> Although this is a civil lawsuit between private parties, the Alabama courts have applied a state rule of law which petitioners claim to impose invalid restrictions on their constitutional freedoms of speech and press. It matters not that that law has been applied in a civil action and that it is common law only, though

[93] *Sullivan*, 376 U.S. 254, 279-80 (emphasis added).

[94] *Jacobs v. New York*, 388 U.S. 431, 437 (1967) ("Over and over again we have stressed that First Amendment rights need 'breathing space to survive' and we have been watchful lest coercive measures exercise an *in terrorem* effect which intimidates people from exercising their First Amendment rights. ").

> supplemented by statute. The test is not the form in which state power has been applied but, whatever the form, whether such power has in fact been exercised.[95]

Thus, the broad, tort-like "recklessness" civil liability created by the EARN IT Act will be no less subject to First Amendment scrutiny — and the Fifth Amendment's Due Process protections, which are triggered by burdens on speech rights — than is defamation law.[96]

C. How the EARN IT Act Burdens the First Amendment Rights of Websites

The EARN IT Act violates the First Amendments rights of ICS providers in multiple ways.

Depriving them of an Audience/Users. When the Third Circuit struck down COPA, it noted not only that "many users who are not willing to access information non-anonymously will be deterred from accessing the desired information," but also that this would affect the First Amendment rights of website owners, would be "deprived of the ability to provide this information to those users."[97] The same would be true for the EARN IT Act: ICS providers will be deprived of the ability to facilitate discussions among users who are not comfortable identifying themselves (for age verification) or using inherently insecure services; or to facilitate discussions between adult users and minors.

Limiting Websites' Editorial Discretion. The First Amendment protects the editorial discretion of newspapers broadly, as to both the content and form of their publication. *Miami Herald Publ'g Co. v. Tornillo*, 418 U.S. 241, 258 (1974)("The choice of material to go into a newspaper and the decisions made as to limitations on the size and content of the paper, and treatment of public issues and public officials — whether fair or unfair — constitute the exercise of editorial control and judgment."). In striking down the CDA, the Supreme Court ruled that websites enjoy the same protection: "our cases provide no basis for qualifying the level of First Amendment scrutiny that should be applied to this medium." *Reno*, 521 U.S. at 870. Lower courts have repeatedly relied on *Miami Herald* in upholding the editorial

---

[95] *Id*. at 265.

[96] The First Amendment law's handling of civil liability in general has been called "incoherent." Daniel J. Solove & Neil M. Richards, *Rethinking Free Speech and Civil Liability*, 109 Colum. L. Rev. 1650, 1654 (2009). While these academics lament that "the First Amendment provides little to no restrictions when [contract and property law] restrict speech," they note that "tort law implicates the First Amendment under modern constitutional jurisprudence." *Id*. at 1660.

[97] *Mukasey*, 534 F.3d at 196 (citing *American Civil Liberties Union v. Gonzales*, 478 F. Supp. 2d 775, 806 (E.D. Pa. 2007)).

discretion of websites.[98] In *Bernstein v. United States Dept. of Justice*, 176 F.3d 1132, 1146 (9th Cir. 1999), which struck down export controls on encryption code as an impermissible prior restraint, the Ninth Circuit recognized source code as fully protected speech.[99] As such, decisions made about the code used to configure a website will treated integral to the operation of the website — like decisions about the "size and content" of a newspaper.[100]

Prior Restraint. The EARN IT Act functions as a prior restraint on websites' speech,[101] and "prior restraints on speech and publication are the most serious and least tolerable infringement on First Amendment rights."[102] The Ninth Circuit found struck down export controls on encryption that required Bernstein, a college professor and cryptography expert, to modify academic presentations of his work by modifying written code (expression) and refrain from discussing it in public.[103] The fact that code is functional does not remove it from the realm of speech.[104] Encryption code does more than operate software: it communicates the identity of the parties exchanging messages. Encryption keys represent statements by the providers that a particular message was sent by a user, which brings with it certain security expectations and guarantees. For example,

> In [Apple's] iMessage interface, messages displayed on a blue background indicate that they were sent over the iMessage service, complete with the security guarantees of the service. In contrast, messages displayed on a green background were sent on the "short message service" (SMS), which is the standard "texting" protocol that features no security guarantees.[105]

---

[98] *See, e.g., La'Tiejira v. Facebook, Inc.,* 272 F. Supp. 3d 981, 991 (S.D.Tex. 2017) (La'Tiejira's claims arise directly and exclusively from Facebook's First Amendment right to decide what to publish and what not to publish on its platform).

[99] *Bernstein*, 176 F.3d at 1141. *See also Bernstein v. United States Dep't of State*, 922 F. Supp. 1426, 1439 (N.D. Cal. 1997).

[100] The operation of websites may also additional protection under the Press Clause of the First Amendment. "The Framers' intended the Clause to create a Constitutional protection for enabling unencumbered spaces of *private* communication, free from government surveillance and retribution. Or as Justice Douglas stated, the Clause was designed 'to take Government off the backs of people.'" D. Victoria Baranetsky, *Encryption and the Press Clause*, 6 N.Y.U J. Intell. Prop. & Ent. L. 179, 231 (2017).

[101] Andrew Crocker & Nate Cardozo, *Deep Dive into Crypto "Exceptional Access" Mandates: Effective or Constitutional – Pick One*, Electronic Frontier Foundation (Aug. 13, 2015), https://www.eff.org/deeplinks/2015/08/deep-dive-crypto-exceptional-access-mandates-effective-or-constitutional-pick-one

[102] *Nebraska Press Ass'n v. Stuart*, 427 U.S. 539, 559 (1976).

[103] *Bernstein*, 176 F.3d at 1138-45; *Bernstein*, 922 F. Supp. at 1435.

[104] 922 F. Supp. at 1439.

[105] Leonid Grinberg, Note, *End to End Authentication: A First Amendment hook to the Encryption Debate*, 74 N.Y.U. Ann. Surv. Am. L. 173, 204 n.105 (2018).

Courts have protected as speech far less communicative expressions, such as upholding a merchant's ability to communicate price stickers.[106] Given that encryption keys safeguard how we may speak freely or securely with each other, the EARN IT Act will impermissibly prevent providers from being able to say, truthfully, their communication is secure or private[107] — an additional form of prior restraint.

Compelling Speech. Attempts to modify speech to suit a certain government message has been found to be compelled speech,[108] — for example, forcing "professional fundraisers disclose to potential donors, before an appeal for funds, the percentage of charitable contributions collected during the previous 12 months that were actually turned over to charity."[109] Likewise, as Bob Corn-Revere, veteran First Amendment litigator notes, [i]f you force someone to create a program, you are compelling speech, and compelled speech is no different from banning speech in First Amendment terms."[110] Andrew Crocker and Jamie Williams of the Electronic Frontier Foundation summarize the First Amendment problem:

> Apple is being forced to actually write and endorse code that it—rightly—believes is dangerous. And in doing so, it is being forced to undermine the trust it has established in its digital signature. The order is akin to the government forcing Apple to write a letter in support of backdoors and sign its forgery-resistant name at the bottom. [111]

D. The EARN IT Act Imposes an Unconstitutional Condition on the Exercise of Editorial Discretion.

Politicians of both parties insist that Section 230 is a special privilege granted only to "Big Tech." This is false: the law applies equally to *all* ICS providers, from the largest social media service to the smallest blog, protecting traditional media services like broadcasters and newspapers from liability for user comments posted on sites in exactly the same way that it

---

[106] *Expression Hair Design v. Schneiderman*, 137 S. Ct. 1144, 1147 (2017).

[107] Grinberg, *supra* note 103, at 199.

[108] *Turner Broad. Sys., Inc. v. FCC*, 512 U.S. 622, 655 (1994).

[109] *Riley,* 487 U.S. at 795.

[110] Cynthia Brumfield, *US Department of Justice push for encryption backdoors might run afoul of First Amendment*, CSO (Nov. 4, 2019) https://www.csoonline.com/article/3450020/us-department-of-justice-push-for-encryption-backdoors-might-run-afoul-of-first-amendment.html]

[111] Andrew Crocker & Jamie Williams, *Deep Dive: Why Forcing Apple to Write and Sign Code Violates the First Amendment*, Electronic Frontier Foundation (March 3, 2016), https://www.eff.org/deeplinks/2016/03/deep-dive-why-forcing-apple-write-and-sign-code-violates-first-amendment,.

protects ICS providers for user content, chat services for messages sent between users, and photo and video services for the content posted by their users.

Sponsors of the EARN IT Act claim that withholding such a "subsidy" does not violate the First Amendment. This is clearly wrong. The Supreme Court has clearly barred the government from forcing the surrender of First Amendment rights in order to qualify for a benefit or legal status. In 2013, the Supreme Court held that the government cannot condition the receipt of AIDS-related funding on the recipients' adoption of a policy opposing prostitution (a form of compelled speech). [112] Fifty years earlier, the Court made it clear that denying a tax exemption to claimants who engage in certain forms of speech effectively penalizes them for that speech — essentially fining them for exercising their First Amendment rights. [113] Using Section 230 to coerce social media companies into surrendering their First Amendment rights, or compromising the First Amendment rights of their users, is no different.

E. Criminalizing the Enforcement of Certifications Amplifies the Bill's First Amendment Problems.

Section 5 of the EARN IT Act makes it a criminal offense, punishable by up to two years' imprisonment, to "knowingly submit a written certification under section 4(d) that contains a false statement." This raises three First Amendment problems. First, note its wording: "knowing" modifies "submits" rather than modifying "false statement." Compare that with 18 U.S.C. § 1001 (Statements or entries generally), which punishes any person who:

> knowingly and willfully—
>
> (1) falsifies, conceals, or covers up by any trick, scheme, or device a material fact;
>
> (2) makes any materially false, fictitious, or fraudulent statement or representation; or

[112] *Agency for Int'l Dev. v. All. for Open Soc'y Int'l, Inc.*, 570 U.S. 205 (2013).

[113] *Speiser v. Randall*, 357 U.S. 513, 518 (1958); *see also Elrod v. Burns*, 427 U.S. 347, 363 (1976) ("if conditioning the retention of public employment on the employee's support of the in-party is to survive constitutional challenge, it must further some vital government end by a means that is least restrictive of freedom of belief and association in achieving that end, and the benefit gained must outweigh the loss of constitutionally protected rights"); *Sherbert v. Verner*, 374 U. S. 398, 374 U. S. 404 (1963) ("It is too late in the day to doubt that the liberties of religion and expression may be infringed by the denial of or placing of conditions upon a benefit or privilege.").

> (3) makes or uses any false writing or document knowing the same to contain any materially false, fictitious, or fraudulent statement or entry.

Under Section 1001, it is clear that the defendant must know the statement at issue was false. By contrast, under the EARN IT Act, an executive of an ICS provider could be prosecuted for submitting a certification containing false statements, regardless of whether the executive knew that the statements were false. This would clearly violate the First Amendment: "[E]ven when the utterance is false, the great principles of the Constitution which secure freedom of expression ... preclude attaching adverse consequences to any except the knowing or reckless falsehood."[114]

In *United States v. Alvarez,* the Court struck down a statute criminalizing false claims that a person had been awarded the Congressional Medal of Honor, noting that there is no "general exception to the First Amendment for false statements," "[a]bsent from those few categories where the law allows content-based regulation of speech."[115] The government invoked 18 U.S.C. § 1001 as one of three "examples of regulations on false speech that courts generally have found permissible: first, the criminal prohibition of a false statement made to a Government official, 18 U.S.C. § 1001; second, laws punishing perjury; and third, prohibitions on the false representation that one is speaking as a Government official or on behalf of the Government."[116] The Court clearly indicated that Section 1001 was constitutional, stating that this "does not lead to the broader proposition that false statements are unprotected when made to any person, at any time, in any context."[117]

The second, crucial difference between Section 1001 and the EARN IT Act is that the latter requires that the misstatement be *material*. [118] Likewise, perjury requires a showing of materiality, as Justice Breyer (joined by Justice Kagan) noted in his concurrence. The third category of false statements that may be criminalized can also be distinguished from the EARN IT Act: "statutes forbidding impersonation of a public official typically focus on acts of impersonation, not mere speech, and may require a showing that, for example, someone was

---

[114] *Garrison v. Louisiana*, 379 U.S. 64, 73 (1964). "Calculated falsehood falls into that class of utterances which 'are no essential part of any exposition of ideas, and are of such slight social value as a step to truth that any benefit that may be derived from them is clearly outweighed by the social interest in order and morality….' Hence the knowingly false statement and the false statement made with reckless disregard of the truth, do not enjoy constitutional protection. *Id*. at 75 (quoting *Chaplinsky* v. *New Hampshire*, 315 U.S. 568, 572 (1942)).

[115] 567 U.S. 709, 718 (2012).

[116] *Id*. at 720.

[117] *Id*. at 735 (Breyer, J. concurring)

[118] *Id*. at 734 (Breyer, J. concurring) (citing 18 U.S.C. § 1621).

deceived into following a 'course [of action] he would not have pursued but for the deceitful conduct.'"[119] Influencing the actions of others is, effectively, what materiality means. By not including a materiality requirement, the EARN IT Act allows criminal prosecutions, punishable by up to two years in prison, for technical, immaterial violations. In this sense, the EARN IT Act is far more draconian than, say, the Sarbanes-Oxley Act, which requires certification by executives of financial reports, but also punishes only materially false statements.[120]

Even if both of these problems were fixed through amendment, a third, more fundamental problem would remain. The EARN IT Act is clearly modeled on the kind of certification regime used to enforce Sarbanes-Oxley. But the bill is considerably more constitutionally problematic because, instead of requiring certification to specific rules governing their business conduct, the EARN IT Act requires certification with vague "best practices" that govern how social media companies exercise their editorial discretion (which the First Amendment protects) in ways that affect the speech rights of their users (which are even more clearly protected speech). The First Amendment problems inherent in such a scheme would be obvious if it were applied to traditional media: If the government offered newspapers and broadcasters a subsidy contingent on their compliance with a set of nominally voluntary "best practices," the ability to incarcerate media executives because the government determined that the company's interpretation of an ambiguous practice would be understood for what it is: a tool for compelling executives to have their companies do the government's bidding, lest those executives risk incarceration. This is censorship of the worst kind.

IV. The Earn It Act Violates the Constitution's Separation of Powers.

The EARN IT Act takes a completely novel approach to making what amounts to law, one that subverts the separation of powers at the heart of our constitutional order.

A. The Bill Was Modified Before Introduction to Avoid Nondelegation Problems, but to No Avail.

The initial version of the bill, leaked in January, raised a glaring separation of powers problem: the bill simply outsourced the drafting of what amounts to *de facto* regulations — with serious First and Fourth Amendment implications — to a private body. This would

[119] *Id*. at 735 (Breyer, J. concurring).

[120] Sarbanes-Oxley Act of 2002, 15 U.S.C. § 7201 et seq. (2002); 15 U.S.C. § 7241 (Section 302) (civil provision); 18 U.S.C. § 1350 (Section 906) (criminal provision).

clearly violate the nondelegation doctrine: "Congress is not permitted to abdicate or to transfer to others the essential legislative functions with which it is thus vested."[121] The Supreme Court struck down three major pieces of New Deal legislation under the doctrine, including both delegation to regulatory agencies with insufficiently clear standards[122] and delegation to industry bodies.[123]

Though essentially treated as dead since the "switch in time that saved nine" (the 1937 shift on the Court in response to President Roosevelt's Court-packing scheme[124]), the Supreme Court's decision last year in *Gundy v. United States* clearly signaled that a majority of the Court is now ready to revive the nondelegation doctrine. Congress had passed a new sex offender law and gave the Attorney General the authority to "specify the applicability" of a certain provision of the law to "sex offenders convicted before" the date of the law's enactment.[125] The four liberal justices voted to uphold the law, while the Chief Justice and Justices Gorsuch and Thomas voted to strike it down under the nondelegation doctrine. But Justice Kavanaugh recused himself from the case because oral arguments took place the day before his inauguration to the Court.[126] Justice Alito, concurring only in the judgment, wrote, "[i]f a majority of this Court were willing to reconsider the approach we have taken for the past 84 years, I would support that effort."[127] In another case several months later, Justice Kavanaugh, to no one's surprise, clearly signaled his willingness to revive the nondelegation doctrine.[128] This means that, despite the holding in *Gundy*, there is now a clear majority on the court for reviving the nondelegation doctrine.[129]

---

[121] *A.L.A. Schechter Poultry Corp. v. United States*, 295 U.S. 495, 529 (1935).

[122] *Panama Refining Co. v. Ryan*, 293 U.S. 388, 430 (1935).

[123] *Carter v. Carter Coal Co.*, 298 U.S. 238, 311 (1936); *Schechter*, 295 U.S. 495, 537 (1935).

[124] Lesley Kennedy, *This is How the FDR Tried to Pack the Supreme Court*, History (June 28, 2018) https://www.history.com/news/franklin-roosevelt-tried-packing-supreme-court.

[125] *Gundy v. United States*, 139 S. Ct. 2116, 2121 (2019).

[126] *Id.* at 2130.

[127] *Id.* at 2131 (Alito, J., concurring).

[128] *Paul v. United States,* 140 S. Ct. 342 (2019) (mem.) (Kavanaugh, J., statement respecting the denial of certiorari) (stating that the issues raised in the *Gundy* dissent "may warrant further consideration in future cases").

[129] Mila Sohoni, *Opinion analysis: Court refuses to resurrect nondelegation doctrine*, SCOTUSBlog (June 20, 2019), https://www.scotusblog.com/2019/06/opinion-analysis-court-refuses-to-resurrect-nondelegation-doctrine; Following Justice Kavanaugh's appointment and discussing *Gundy*, "… there are now five conservative constitutionalists on the Court who will, for the first time, be able to reinvigorate the non-delegation doctrine" Peter Wallison, *Rumors of the Non-Delegation Doctrine's Demise are Greatly Exaggerated*, Law & Liberty (June 26, 2019).

While the issue in *Gundy* involved delegation to the Attorney General, delegations to quasi-public or private bodies would raise even greater nondelegation concerns, since it outsources an essentially legislative function to a private body (dominated by the Attorney General). As the Court said in *Carter Coal* of a similar delegation to an informal, non-governmental body, "This is legislative delegation in its most obnoxious form, for it is not even delegation to an official or an official body… but to private persons…."[130] Justice Gorsuch's *Ackerman* opinion (while sitting on the Tenth Circuit) provides additional reason to expect the Court to find a nondelegation problem in a system that essentially "delegates" authority to a private body to make requirements to compel private companies to collect evidence in warrantless searches.[131]

For Congressional Republicans, the fact that the Court has not *yet* revived the nondelegation doctrine should be immaterial; doing so has been among the very top priorities of Republican legal experts for years.[132] Thus, it is perhaps unsurprising that the most substantial change Sen. Graham made to the bill prior to introduction was the addition of a requirement that the Commission's "Best Practices" would have to be approved by both chambers of Congress. If, this change was intended to solve the nondelegation problem, it fails — and creates an entirely new constitutional problem: violating the presentment clause by which a bill normally becomes a law.

B. The Congressional Approval Process for Best Practices May Violate the Constitution's Presentment Clause.

The best practices issued by the Commission clearly have the force of law: even if Courts do not consider them tantamount to legal mandates that directly compel changes to ICS providers' operation, they clearly become conditions of Section 230 immunity, thus effectively amending Section 230. Thus, the bill creates a bespoke procedure by which Congress, relying on a quasi-governmental body, bypasses "the express procedures of the Constitution's prescription for legislative action: passage by a majority of both Houses and presentment to the President." *Immigration and Naturalization Service v. Chadha,* 462 U.S. 919, 958 (1983). This violates the Constitution's "Presentment Clauses," Art. I, § 7, cls. 2, 3,

[130] *Carter Coal*, 298 U.S. at 311.

[131] *See infra* note 47 and associated text.

[132] Judge Janice Rogers Brown's (a conservative hero shortlisted for the Supreme Court) opinion for the unanimous panel called the regulatory structure created by Congress "as close to the blatantly unconstitutional scheme in *Carter Coal* as we have seen." *Ass'n of Am. R.R. v. Dep't of Transp.*, 721 F.3d 666, 673 (D.C. Cir. 2013); Adam White, *Congress and the New Administrative State*, The Heritage Foundation (May 22, 2014), https://www.heritage.org/government-regulation/report/congress-and-the-new-administrative-state.

for the same reasons the Court struck down the line-item video in *Chadha*. "The division of the Congress into two distinctive bodies assures that the legislative power would be exercised only after opportunity for full study and debate in separate settings."[133] The Court harkened back to the Framing of the Constitution in terms that Republicans, as professed originalists, should find impossible to ignore: "The choices we discern as having been made in the Constitutional Convention impose burdens on governmental processes that often seem clumsy, inefficient, even unworkable, but those hard choices were consciously made by men who had lived under a form of government that permitted arbitrary governmental acts to go unchecked."[134]

There is, of course, one easy way to solve this constitutional problem: amend the EARN IT Act so that the bill convenes an expert Commission to make recommendations to Congress on how to modify Section 230's liability shield, which would then have to be enacted in a subsequent piece of legislation approved by both chambers and signed by the President. But this would be difficult — far more difficult than passing the EARN IT Act, since such a bill would make clear the true implications for users' privacy and speech rights. Thus, the EARN IT Act simply avoids the need for such monumental decisions to be made through the constitutionally prescribed legislative process — allowing the Attorney General, in effect, to decide these matters. The bill's current structure also allows its sponsors to maintain the smoke screen that these decisions are being made through the Commission, and that this is unproblematic, constitutionally, because the Commission is merely making recommendations as to "voluntary" "Best Practices. Amending the bill to avoid both nondelegation and presentment problems would lay bare what is really happening: conditioning of Section 230 immunity on compliance with these *requirements* (a) may convert providers into government actors for Fourth Amendment purposes and (b) may violate the First Amendment "unconstitutional conditions" doctrine.

The EARN IT Act appears to be modeled on the Congressional Review Act,[135] which allows Congress to block legislative rules issued by administrative agencies. The fact that the CRA has not been subject to constitutional challenge may seem to offer hope for the EARN IT Act, but note two key differences. First, unlike the EARN IT Act, a CRA resolution of disapproval *does* require either the signature of the president or overcoming a presidential veto (or

[133] 462 U.S. at 951.

[134] *Id.* at 959.

[135] 5 U.S.C. § 801 *et seq*.

pocket veto).[136] Second, CRA allows Congress to *block* regulations issued by agencies while the EARN IT Act would allow Congress to *create* legislative rules of its own without the Executive Branch. Under the CRA, the ultimate legislative power remains with Congress; under the EARN IT Act, it is ceded to the Commission, and thus the Executive Branch.

C. The Fast Track Process May Violate the Nondelegation Doctrine or Raise Other Constitutional Concerns.

While the EARN IT Act requires both the House and Senate to approve the "Best Practices" resolution developed by the Commission and "approved" by the Attorney General, it denies lawmakers the opportunities to shape the outcome afforded by the normal procedure for legislating. Instead, EARN IT requires that the lawmakers follow a "fast track" process modeled on that contained in Trade Promotion Authority, which bars *all* amendments.[137] The EARN IT Act bars amendments only on the House or Senate floor, not in Committee. This allows EARN IT's sponsors to claim that Congress would not cede ultimate control over the substance of a "Best Practices" resolution.

In practice, however, EARN IT Act is designed to ensure that these resolutions sail through committee and are subject only to an up or down vote on the floor of each chamber. That's because the bill provides that, if the House or Senate committee to which a resolution is referred fails to discharge the resolution within 45 days, the resolution is automatically referred to the House or Senate floor.[138] This means that the chairmen of these two Committees can deny other lawmakers their *only* opportunity to propose amendments to such a bill simply by choosing not to schedule a markup of the bill. Given the political toxicity of this issue, it is nearly impossible to imagine a committee chairman of either party risking their political career by tying up the passage of a resolution framed as a vital measure necessary to stop the scourge of CSAM. This procedure is designed for one clear purpose: to assure that the "Best Practices" many tech companies will, in practice, be required to follow are determined by the Commission and the Attorney General, rather than the elected representatives of the American people. In other words, behind the Fast Track procedure lurks the exact same nondelegation problem that seemed to have been solved by giving

[136] 5 U.S.C. § 801(e) & 802(a). "A joint resolution of disapproval requires signatures of the President to become law… A two-thirds majority of both houses of Congress is required to override a President's veto." U.S. Congressional Research Service, The Congressional Review Act (CRA): Frequently Asked Questions (R43992; Jan. 14, 2020) at 5.

[137] 19 U.S.C. § 2191(d) ("No amendment to an implementing bill or approval resolution shall be in order in either the House of Representatives or the Senate.").

[138] EARN IT Act §§ 4(c)(4)(A) & (c)(5)(A).

Congress a role in finalizing a Best Practices resolution — because that role turns out to be perfunctory at best, and illusionary at worst.

D. The "Reasonableness" Backstop Presents a Harder Nondelegation Problem.

Recall that certifying compliance with the "Best Practices" is not the only way to regain Section 230 protections. An ICS provider may instead establish the "reasonableness" of its practices in civil litigation under Section 2255. But when a court makes an assessment of reasonableness, it is difficult to imagine that such an assessment will not be informed — indeed, dominated — by the Best Practices developed by the Commission and published by the Attorney General. Even if these have not been finalized through the EARN IT Act's congressional approval procedures, or while that process is pending, such "best practices" may irrevocably tilt the evidentiary scales in litigation such as to have the force of law. They will have been published in the Federal Register,[139] and while this alone does not give them force of law, it is difficult to imagine that a court will not consider such a document in assessing the reasonableness of a company's practices.

V. The EARN IT Act Bypasses the Normal Safeguards of Notice-and-Comment Rulemaking.

The Commission created by the EARN IT Act would make *de facto* rules but without the procedural safeguards of the Administrative Procedure Act of 1946,[140] which reflect Congress's decision that public participation in the rulemaking proceedings of increasingly powerful agencies is essential to protect due process interests. Most notably, at no point in the process established by the bill would the public have the opportunity to comment on the "best practices" developed by the Commission, as the APA requires when an administrative agency makes a rule equivalent to these "best practices." The importance of providing the opportunity for notice and comment was highlighted by the Court in *Office of Communication of United Church of Christ v. F.C.C.*, which described it as part of the "national tradition that public response is the most reliable test of ideas."[141] The EARN IT Act clearly violates the spirit, if not the letter, of the APA.

---

[139] EARN IT Act § 4(b)(1)(B)(i).

[140] 5 U.S.C. ch. 5, subch. II § 551 *et seq*.

[141] 359 F.2d 994, 1003 (D.C. Cir. 1966).

VI. Conclusion

There is no more vile crime than the sexual exploitation of children — a crime that continues with each viewing of the imagery of such abuse. The EARN IT Act invokes outrage about such abuse, but does *nothing* to address the chronic under-funding of enforcement of existing laws against CSE and CSAM. Despite pleas that federal prosecutors are under-resourced, Congress has spent half as much money on state and local CSAM enforcement as it allocated back in 2008.[142] The Attorney General *could* have deputized state, local and tribal prosecutors to enforce Sections 2252 and 2252A under clear legal authority,[143] but has failed to so do. Indeed, instead of increasing funding, the Trump administration actually has raided the cybercrime budget to pay for immigration enforcement.[144] The Department of Justice has not even bothered to issue three of the last five biennial reports on CSAM enforcement since 2008, and the two reports it did issue failed to include crucial data, such as trade in CSAM images.[145] If anything, the EARN IT Act could actually make law enforcement's job significantly harder by ending today's close cooperation between law enforcement and tech companies.

In short, the sponsors of the EARN IT Act are cynically using CSAM and CSE as a pretext for a much broader agenda: limiting Americans' right to use truly secure tools for their most private communications, to use such tools anonymously, and to communicate with other users of all ages. The bill's Rube-Goldberg-esque structure reflects a calculated attempt to conceal the coercive nature of the bill, and circumvent both the First and Fourth Amendment. As if this were not bad enough, the bill upends completely the Constitution's process for making law. There is simply no way to reconcile the bill with the Constitution the Founders gave us. If the bill does become law, it will be struck down in court just as were the Communications Decency Act of 1996 and the Child Online Protection Act of 1998. This

---

[142] Michael H. Keller & Gabriel J.X. Dance, *The Internet Is Overrun With Images of Child Sexual Abuse. What Went Wrong?*, NY TIMES (Sept. 29, 2019), https://www.nytimes.com/interactive/2019/09/28/us/child-sex-abuse.html ("Congress has regularly allocated about half of the $60 million in yearly funding for state and local law enforcement efforts.").

[143] 28 U.S.C. § 543(a) ("The Attorney General may appoint attorneys to assist United States attorneys when the public interest so requires").

[144] Keller, *supra* note 141, ("Separately, the [DHS] this year diverted nearly $6 million from its cybercrime units to immigration enforcement – depleting 40 percent of the units' discretionary budget…").

[145] *Id*. ("Another cornerstone of the law, the biennial strategy reports by the Justice Department, was mostly ignored. Even the most recent of the two reports that were published, in 2010 and 2016, did not include data about some of the most pressing concerns… In 2011, the [GAO] reported that no steps had been taken to research which online offenders posed a high risk to children, and that the Justice Department had not submitted a progress assessment to Congress, both requirements of the law").

might serve the political objectives of the bills' sponsors, but it will do nothing to protect children.