March 5, 2020

The Honorable Lindsey Graham
Chairman, Senate Judiciary Committee
United States Senate
290 Russell Senate Office Building
Washington, D.C. 20510

The Honorable Diane Feinstein
Ranking Member, Senate Judiciary Committee
United States Senate
331 Hart Senate Office Building
Washington D.C. 20510

Re: The Eliminating Abusive and Rampant Neglect of Interactive Technologies Act of 2020 (the "EARN IT Act") S.___

Dear Chairman Graham, Ranking Member Feinstein, and members of the Senate Judiciary Committee:

We write to express our concerns about the EARN IT Act.[1] We take seriously the need to do more to stop the spread of child sexual abuse material (CSAM) and other child sexual exploitation (CSE) content over the Internet. But as drafted, this bill fails to address the most pressing needs of law enforcement, could actually make the fight against CSAM and CSE harder, and is written so broadly that it could be used not to crack down on criminals, but to compromise the security of online communications tools used by law-abiding Americans and invade their privacy — *e.g,.* by effectively banning "strong" end-to-end encryption, mandating extensive data retention, and requiring sweeping age-verification of adults.

We do not believe that protecting children online requires undermining the security of online communications tools or amending Section 230, the law that has made such services — and the rest of today's Internet — possible. The obvious intent of the EARN IT Act is to use the indispensability of Section 230 protections to coerce ICS providers into complying with "best practices" as *de facto* regulatory mandates that could go far beyond CSAM or CSE.

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

Such mandates could convert countless private entities into "government actors" for Fourth Amendment purposes, which would utterly destroy the current CSAM reporting system.

There is a real and urgent problem: neither Congress nor this administration nor the previous administration have made it a priority to enforce existing laws against CSAM and CSE. Congress has spent just half the money on CSAM/CSE enforcement that it promised to spend in 2008.[2] The Department of Justice has failed to produce three of the five biennial reports Congress required it to produce in 2008.[3] Most outrageously, the Trump administration has raided money from the Department of Homeland Security's cybercrime budget to spend on immigration enforcement.[4] The EARN IT Act would do nothing to remedy these problems. If lawmakers are serious about protecting children, they must start here — and they will have our full support in doing so.

In 2018, we worked closely with the staff of House Judiciary Committee Chairman Bob Goodlatte and Rep. Ann Wagner to craft a new federal criminal statute targeted to the facilitation of online prostitution. The result, a revised version of the Fight Online Sex Trafficking Act (FOSTA) earned our public support.[5] We opposed marrying that bill to SESTA, the Senate bill.[6] The House bill did not require amending Section 230 because it created a new federal criminal law, and Section 230 has *never* protected interactive computer service (ICS) providers (*e.g.*, operators of websites, messaging services, video or file-sharing services) from prosecution under federal criminal law.

The EARN IT Act is more like SESTA than FOSTA: rather than modify federal criminal law, the bill would work by making two amendments to Section 230:

---

[2] Michael H. Keller & Gabriel J.X. Dance, T*he Internet Is Overrun With Images of Child Sexual Abuse. What Went Wrong?*, N.Y. Times (Sept. 29, 2019), https://www.nytimes.com/interactive/2019/09/28/us/child-sex-abuse.html.

[3] *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, such as the trade in illicit imagery.)

[4] Andy Sullivan, *Trump administration taps disaster, cyber funds to cover immigration*, Reuters (Aug. 27, 2019), https://www.reuters.com/article/us-usa-immigration-funds/trump-administration-taps-disaster-cyber-funds-to-cover-immigration-idUSKCN1VH2F7.

[5] Letter, To Rep. Goodlate and Rep. Wagner Re Fosta Markup, TechFreedom (Dec. 11, 2017), *available at* https://techfreedom.org/wp-content/uploads/2017/12/TechFreedom-Letter-FOSTA-Markup-12.11.17-1.pdf

[6] Merging SESTA & FOSTA Would Harm, Not Help, Trafficking Victims, TechFreedom (Feb. 23, 2018), https://techfreedom.org/merging-sesta-fosta-harm-not-help-trafficking-victims/.

1. ICS providers would become liable for prosecution under state criminal laws "if the conduct underlying the charge would constitute a violation of" the two federal CSAM and CSE statutes, 18 U.S.C. §§ 2252 & 2252A.[7]
2. ICS providers could face potentially business-ending civil liability in lawsuits filed by those depicted in CSAM/CSE images or videos under 18 U.S.C. § 2255.[8]

The bill also amends 18 U.S.C. § 2255 to lower the standard of evidence required in those civil lawsuits such that plaintiffs would only have to show that an ICS provider acted "recklessly," not that they had "actual knowledge" of CSAM or CSE material.[9] ICS providers could "earn" back Section 230 protections against such liability (and prosecution under state criminal laws) if they certify their compliance with the "best practices" recommended by an expert Commission created by the bill.[10] We have three related concerns:

1. The new legal liability created under 18 U.S.C. § 2255 is much too broad. ICS providers could be sued not merely for failing to police CSAM/CSE content perfectly, or to report it to NCMEC in particular ways, but for making decisions to offer privacy-protective features with enormous benefits for law-abiding users. If ICS providers face sufficient legal risk for offering strong encryption or limiting the period for which they retain user data, that risk will force them to re-engineer their services even without any specific commandment from the government, a court or an expert commission that they do so.
2. The bill's amendments to 18 U.S.C. § 2255A and Section 230 would take effect one year after the best practices issued by the Commission go into effect — or, if such best practices have not yet been finalized, within four years.[11] In the latter situation, ICS providers would have to show that they have "implemented reasonable measures relating to the matters [covered by the bill's provision governing best practices]."[12] Likewise, once the Commission finally issues its "recommendations," an ICS provider would have to certify compliance with *all* of the Commission's "best practices" in order to reclaim Section 230 protections. This could be even more difficult than making such a showing before the "best practices" are issued: any divergence between a company's practices and the Commission's recommendations could be treated as presumptively unreasonable. Requiring defendants establish the "reasonableness" of their practices before availing themselves of Section 230's safe

[7] EARN IT Act § 6(a)(6)(A)(ii) (2020).

[8] *Id.* at § 6(a)(6)(A)(i).

[9] *Id*. at § 6(b)(3).

[10] *Id.* at § 6(a)(6)(B)(i).

[11] *Id*. at § 6(c)(1)(B).

[12] *Id.* at § 6(a).

harbor (with a motion to dismiss filed under Fed. R. Civ. Pro. 12(b)(6)) would make the safe harbor functionally useless for most small ICS providers. Establishing "reasonableness" will require providers to spend enormous sums of money litigating cases to final judgment in order to defeat even meritless claims that they would previously have been able to dismiss on the pleadings with relatively minimal legal expenses (though, for smaller ICS providers, even small expenses could be large enough force them to have no choice but to comply with the Commission's "best practices").

3. The bill uses the indispensability of Section 230 protections to coerce ICS providers into complying with "best practices" as *de facto* regulatory mandates that could go far beyond CSAM or CSE. That might mean restricting encryption or mandating data retention, but it could also include other things, such as "employing age rating and age gating systems"[13] and "offering parental control products that enable customers to limit the types of internet websites and content accessible to children."[14]

I. Fourth Amendment Concerns About the EARN IT Act's Structure

While most of the attention paid to the bill thus far has centered on encryption, many advocates of the bill have disclaimed any intention to use the bill to restrict encryption. Last summer, the National Center for Missing and Exploited Children (NCMEC) complained to Congress of essentially four problems with the status quo (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."[15] Thus, the nature of reporting to NCMEC varies significantly.
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."[16]
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

[13] *Id.* at § 4(a)(3)(1)(I).

[14] *Id.* at § 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.

[15] 18 U.S.C. § 2258A(b).

[16] *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.

child sex trafficking, but which are common forms of online child sexual exploitation."[17]

4. Some ICS providers do not "proactively search or screen their networks for [CSAM]."[18]

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;[19] thus, the statute continued to require providers to report only CSAM they "obtain[] actual knowledge of." The obvious question one must ask is why Congress crafted, and maintained, a nominally voluntary system — and why the EARN IT Act does not simply mandate any of the "best practices" it contemplates, and, indeed, specifically excludes content filtering from what the "best practices" can cover.[20] The answer is simple but often overlooked: direct mandates could lead a court to decide that ICS providers are "government actors" subject to the Fourth Amendment,[21] just as the Tenth Circuit has ruled that NCMEC, nominally a private non-profit, is a government actor.[22] 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 NCMEC or other government actors.[23] In short, direct mandates could bring the entire system of cooperation between ICS providers and law enforcement crashing down. Individuals convicted 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.

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.

Conditioning Section 230 immunity against significantly increased CSAM liability on compliance with "best practices" developed by a commission operating under the

---

[17] *Id*.

[18] *Id*.

[19] 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.

[20] EARN IT Act § 9.

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

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

[23] Mitter, *supra* note 21.

supervision and, effectively, direction of the Attorney General, may be tantamount to issuing direct mandates. As Justice Gorsuch, then a Tenth Circuit judge, explained in *Ackerman*, circuit courts have varied in the tests they have applied for determining when a nominally private actor is operating as a government actor.[24] The First Circuit has considered "[1] the extent of the government's role in instigating or participating in the 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."[25] 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."[26] 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. "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.'"[27] The benefit to the government here is obvious: assisting in the prosecution of CSAM/CSE laws. Furthermore, since the obvious 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 was involved 'directly as a participant . . . or indirectly as an encourager,' then the private actor likely intended his search to assist law enforcement."[28] Using Section 230 as the mechanism of "encouragement" may be considered tantamount to a reward.[29]

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[30] — 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

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

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

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

[27] *United States v. Attson*, 900 F.2d 1427, 1431 (9th Cir. 1990); Mitter, *supra* note 21.

[28] Mitter, supra note 21 at 271 (quoting *United States v. Leffall*, 82 F.3d 343, 347 (10th Cir. 1996)).

[29] *Id*. (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)).

[30] EARN IT Act § 6(a)(6)(B)(i).

little difference to a court's analysis, especially if few ICS providers chose not to certify compliance with the Commission's "best practices."[31]

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. The Fourth Amendment question would have to be raised by an individual criminal defendant whose communications were "searched" *after* the Commission's "best practices" had gone into effect (the bill gives the Commission 18 months[32]). And after a district court rules on this evidence, the case will have to work its way through the appeals process.

In short, the EARN IT Act contains a ticking constitutional time bomb that could take years to explode: it 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.

If, to return to NCMEC's complaints, lawmakers simply want to improve the nature of reporting of CSAM and CSE, and especially if the perceived problem today is inconsistent or inadequate reporting by smaller ICS providers, they should consider increasing funding for the implementation of better reporting. Microsoft has made its PhotoDNA service free for "qualified customers," including not only non-profits but for-profit companies.[33] But the real cost that may cause smaller companies not to use such software is implementation, and specifically, hiring and training the highly specialized employees responsible for dealing with CSAM. While the exact scope of this problem remains unclear, NCMEC is well-positioned to understand, and attempt to remedy, it — provided they are given the funding to do so.

---

[31] In *Ackerman*, the Tenth Circuit cited numerous attempts by the government to cloak a government entity as a private party. "[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." 831 F.3d at 1300 (internal citations omitted)

[32] EARN IT Act § 4(a)(1)(A).

[33] *PhotoDNA*, Microsoft (2020), https://www.microsoft.com/en-us/photodna/faq.

II. Procedural Concerns about the EARN IT Act

We have three concerns about the EARN IT Act's use of a private body to issue *de facto* regulations. The first two are constitutional, while the third is nearly so.

First, again, we understand why it might seem easier to lawmakers to write a law that effectively commands private companies to assist law enforcement — to render them government actors while maintaining the pretense that they are not — than to actually craft a system of cooperation between private companies and the government that satisfies the Fourth Amendment. But the point of drawing a line between private and government actors is to give effect to "the Fourth Amendment value of protecting individuals from unnecessary intrusion by government actors;" that is why these tests "focus on 'whether the governmental involvement is significant or extensive enough to objectively render an otherwise private individual a mere arm, tool, or instrumentality of the state.'"[34] Adopting a legal Rube Goldberg mechanism for coercing private parties to bypass the protections of the Fourth Amendment set a dangerous precedent with implications far beyond CSAM (as well as the risk of a court eventually striking down the entire system of policing CSAM/CSE).

Second, the EARN IT Act could amount to an unconstitutional delegation of law-making powers to a non-governmental organization. Last year, the Supreme Court declined to revive the non-delegation doctrine in *Gundy v. United States*, a case involving the delegation to the attorney general the authority to "specify the applicability" of a certain provision of a new sex offender law to "sex offenders convicted before" the date of the law's enactment.[35] But Justice Alito, concurring only in the judgment, wrote, "If a majority of this Court were willing to reconsider the approach we have taken for the past 84 years, I would support that effort."[36] This means that, despite the holding in *Gundy*, a majority of the Court actually signaled their *support* for reviving the non-delegation doctrine.[37] If granting the Attorney General the power to interpret such a statute violates the non-delegation doctrine, it is difficult to see how granting the Attorney General the power to convene a commission to determine the requirements of accessing a vital protection against legal liability would *not* create an even greater non-delegation problem.

---

[34] Mitter, *supra* note 21 at 272 (quoting State v. Kahoonei, 925 P.2d 294, 300 (Haw. 1996) ("In so doing, we focus on the actions of the government, because . . . the subjective motivation of a private individual is irrelevant.")).

[35] *Gundy v. United States*, No. 17-6086, 588 U.S. ___ (2019).

[36] *Id.* (Alito, J., concurring).

[37] 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.

Finally, the Commission created by the EARN IT Act would make *de facto* rules but without procedural safeguards of the Administrative Procedure Act. Most notably, the public would never have the opportunity to comment on proposals. Nor is it clear when there ever be a "final action" by a government entity that could be challenged in court. The bill's elaborate system by which "best practices" would be presented to Congress for disapproval seems to combine non-delegation problems with the constitutional problems raised by the legislative veto in *Chadha*.[38]

III. Increased Civil Liability under the EARN IT Act

Section 2255 provision currently authorizes victims of Sections 2252 and 2252A to sue anyone convicted of producing, trafficking, or viewing CSAM depicting them for actual damages of up to $150,000 per image/video, *plus unlimited punitive damages*. The EARN IT Act would amend Section 2255 to allow victims to sue ICS providers if their conduct "would violate section 2252 or Section 2252A" — but with one critical change: where these statutes require "actual knowledge" of CSAM, a plaintiff need prove only "recklessness," which is generally defined as "conscious disregard" of "substantial risk of causing harm" to others.[39] Recklessness is not easy to prove in a criminal case, where the standard of proof is "beyond a reasonable doubt," but in a civil case, a plaintiff need only show a "preponderance of the evidence." Given the potential for punitive damages and the scale of the content available on the Internet, combining recklessness with civil liability means that ICS providers face a significant risk that they could be put out of business not merely for failing to police CSAM perfectly, but for how they design their systems — most notably, for their decision to offer end-to-end ("strong") encryption. Perversely, ICS providers would face a much lower bar for liability under Section 2255 ("recklessness") than would actual child predators convicted of creating, disseminating or consuming CSAM ("actual knowledge").

Attorney General Bill Barr has already laid out the legal case for considering the decision to offer strong encryption to be "reckless." Most notably, in a speech last summer, he said:

> 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

[38] *Immigration and Naturalization Service v. Chadha*, 462 U.S. 919 (1983).

[39] *See, e.g., Voisine v. United States*, 136 S. Ct. 2272, 2279 (2016).

> 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.[40]

This is a roadmap for private plaintiffs to sue ICS providers for being "reckless" in deciding to offer strong encryption, not to retain user data, not to age-gate users, *etc*. The fact that DOJ has laid out such a roadmap will significantly increase the *in terrorem* effects of the EARN IT Act: companies, especially small companies, will have to take seriously the risk that they may be sued under precisely this theory for the decisions they make in designing their services — especially the decision to offer strong encryption.

IV. Engaging State, Local & Tribal Prosecutors

Attorney General Barr and others have complained that federal prosecutors alone cannot adequately enforce existing law. This problem has nothing to do with Section 230. Not only is federal law enforcement in this area simply under-funded, but Section 230 would not prevent the enlistment of state, local and tribal prosecutors in enforcing federal law, because Section 230(e)(1) says "[n]othing in this section shall be construed to impair the enforcement …. any … Federal criminal statute" *without regard to who enforces federal law*. New legislation could, of course, do this directly, but he Attorney General already has the power to deputize state, local and tribal prosecutors as "special attorneys" empowered to enforce CSAM law (like any provision of federal law) under 28 U.S.C. § 543 but simply not done so, nor have they requested that the Attorney General do so. Amending Section 230 to allow states to create and enforce their own laws governing CSAM will do nothing to help law enforcement that deputizing state, local and tribal prosecutors to enforce federal law will do. Indeed, the EARN IT Act would do nothing to empower tribal prosecutors.

Section 230 protects ICS providers from suit under state criminal law but maintains the applicability of federal law. This reflected a conscious decision by Congress in 1996 that there should be a uniform body of federal criminal law — and *only* federal criminal law — to govern Internet services. While that body of law may need to be modified as technology

[40] *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.

changes, the decision to maintain a consistent federal body of law remains correct. It is not enough to, as the EARN IT Act does, tie state laws to federal criminal law by setting aside Section 230's protections only if "the conduct underlying the charge would constitute a violation of [federal law]" because this still allows, for example, for significant differences in procedure between state and federal law, which may actually lead to different outcomes.

V. Conclusion

We understand the frustrations of NCMEC, child protection advocates, and law enforcement with the status quo. Indeed, we share many of their concerns. As we did in 2018, in assisting the House Judiciary Committee in revising FOSTA, we stand ready to assist your committee with drafting legislation that would actually help law enforcement combat the scourge of CSAM and CSE online — *without* compromising the security of services used by law-abiding Americans, or invading their Fourth Amendment rights. Specifically, before proceeding with this legislation, we urge the following:

First, your Committee should hold a hearing to explore the state of Fourth Amendment doctrine. If some legitimate complaints about today's voluntary reporting system can be addressed by requiring more detailed or consistent reporting *without* converting ICS providers into government actors, that should avoid the calamity of trying to use Section 230 as a hook for effectively mandating changes to CSAM/CSE reporting practices that may actually be uncontroversial. The greatest problem with the EARN IT Act is that the bill creates a vehicle that could be used to require far more than what NCMEC and law enforcement really need. In addition, even if direct requirements were to convert ICS providers into government actors, it may be possible to craft adequate safeguards in the process of cooperation between ICS providers and NCMEC to satisfy the Fourth Amendment.

Second, Congress must remedy the chronic underfunding of CSAM/CSE enforcement. Providing funding to NCMEC specifically to help facilitate better cooperation with smaller tech companies may also address much of the perceived problems with today's largely voluntary reporting system.

Third, your Committee should ask the Attorney General why he has not exercised his existing legal authority under 28 U.S.C. § 543 to deputize state, local and tribal prosecutors to enforce federal CSAM and CSE laws. There is simply no need to enact new legislation to gain their assistance in this fight.

Finally, the idea behind the EARN IT Act — or at least, the appearance the bill takes upon first inspection — is sound: an expert commission *should* be convened to study the problem of CSAM, and quickly. Such a commission could even recommend best practices for private

companies, and explore how to facilitate better cooperation amongst them and with NCMEC. What we object to is giving those best practices the force of law as *de facto* mandates, and the enormous legal liability the EARN IT Act would create. A bill without those provisions — and increased funding for law enforcement — could be enacted today while Congress explores the harder questions we have raised here. If convened quickly, a true blue-ribbon commission could conclude its work just as the next Congress turns back to this issue. In the interim, more vigorous enforcement of existing law by federal, state, local and tribal prosecutors could go a long way to protect children from exploitation and abuse.

Sincerely,

Berin Szóka, President, TechFreedom
James Dunstan, General Counsel, TechFreedom
Ashkhen Kazaryan, Director of Civil Liberties, TechFreedom