Written Testimony

HEARING BEFORE THE UNITED STATES SENATE

COMMITTEE ON THE JUDICIARY

March 11, 2020

Testimony of Elizabeth Banker

Deputy General Counsel, Internet Association

I. Introduction

Chairman Graham, Ranking Member Feinstein, and members of the Committee, thank you for inviting me to testify at this important hearing today. My name is Elizabeth Banker, and I am Deputy General Counsel of Internet Association.

I would like to begin by thanking you and Senator Blumenthal for the work you have done to make the eradication of child exploitation and abuse a priority for this Committee. I can say unequivocally that this is also a top priority for the companies IA is proud to represent. These horrific crimes against children, our most vulnerable and precious population, are unconscionable. As good corporate citizens and employers of people who are mothers, fathers, grandparents, aunts, uncles, sisters, brothers, and mentors of children, or who otherwise care deeply about the well-being of children, our member companies are committed to fighting alongside victims, their families and advocates, and our elected leaders to combat these vile crimes.

Internet Association is grateful for the opportunity to appear before the Committee today to discuss the work that our member companies undertake to address crimes against children. This is a paramount concern across IA's broad membership. IA represents over 40 of the world's leading internet companies who range in size and business model considerably.

IA is the only trade association that exclusively represents global internet companies on matters of public policy. IA's mission is to foster innovation, promote economic growth, and empower people through the free and open internet. IA believes the internet creates unprecedented benefits for society, and as the voice of the world's leading internet companies, we ensure stakeholders understand these benefits. IA represents the interests of companies including Airbnb, Amazon, Ancestry, DoorDash, Dropbox, eBay, Etsy, Eventbrite, Expedia, Facebook, Google, Groupon, Handy, IAC, Indeed, Intuit, LinkedIn, Lyft, Match Group, Microsoft, PayPal, Pinterest, Postmates, Quicken Loans, Rackspace, Rakuten, Reddit, Snap Inc., Spotify, Stripe, SurveyMonkey, Thumbtack, Tripadvisor, Turo, Twitter, Uber Technologies, Inc., Upwork, Vivid Seats, Vrbo, Zillow Group, and ZipRecruiter.

IA member companies respect laws and prioritize the safety of those who use their services and the general public. In fact, IA members often moderate or remove objectionable content well beyond what the law requires. And all of this activity is made possible by Section 230.

IA shares the Committee's view that abuse and exploitation of children is an urgent problem, requiring an urgent response. It is for this reason that IA is grateful for the opportunity to address the Committee today to urge that immediate, actionable legislative solutions be adopted, without the delays and problems that the The Eliminating Abusive and Rampant Neglect of Interactive Technologies Act (EARN IT Act) would create.

As I will explain, IA has serious concerns that the EARN IT Act would actually undermine the top-priority efforts that IA companies currently undertake to detect and prevent crimes against children. The EARN IT Act would threaten this important work and weaken prosecutions by allowing criminal defendants to argue that the coercive nature of the bill converts companies' now-voluntary detection efforts into warrantless searches by government agents, raising Fourth Amendment issues that block successful prosecution of these crimes. IA urges the Committee to consider, instead, adopting a series of other measures that can be implemented immediately to address areas of concern.

II. IA Member Companies Are Committed To Substantial Efforts To Combat Child Sexual Abuse Material

IA member companies take multi-faceted approaches to combat Child Sexual Abuse Material (CSAM) on their services and in the world. While each company must determine the most effective measures for that company in light of its primary audience, the features of its products, and the technical options presented by its architecture, IA member companies collaborate and share know-how and tools to fight CSAM. As IA is not in a position to discuss the actions any single member company takes, we will focus on providing a high level overview of the types of actions that are taken by IA member companies and the industry as a whole. Before discussing measures taken today, I would like to share a bit of history on how industry engagement on efforts to fight CSAM has evolved during my time working on this issue.

When the original reporting statute was passed in 1998,[1] only one quarter of IA's companies existed. That law was far less sophisticated than today's legal framework and did not designate an entity to receive reports, nor a way that a private company could transmit reports to law enforcement that would not itself result in a criminal violation. The law, the CyberTipline, and the industry landscape have all changed significantly in the last 22 years. Today's efforts by IA members should be viewed as part of a long continuum of technology and internet services that have made this issue a top priority, invested human and technical resources to building systems for reporting and detection, developed teams equipped to respond to law enforcement emergencies around the clock, and provided resources—whether training, donations of technology, or funds—to support continued progress in this fight.

Fourteen years ago, I sat in front of a panel in the House of Representatives to address similar questions regarding the fight against CSAM, though I was then representing a specific

[1] "Protection of Children From Sexual Predators Act of 1998" P.L. 105-314, OCT. 30, 1998.

company, Yahoo!.[2] During that hearing, industry representatives discussed efforts beginning in the early 2000s to use hash values to detect items previously identified as violations, the legal changes needed to allow sharing of hash values among companies and the National Center for Missing and Exploited Children (NCMEC), the creation of the Technology Coalition to bring industry leaders together to combat child exploitation, and supporting changes to the reporting statute to incorporate reporting best practices that had been developed by industry with input from other stakeholders years earlier.

In 2008, the reporting statute was updated through the PROTECT Our Children Act,[3] and a number of other critical legal changes were made, such as providing legal protection for providers to allow them to send the actual image being reported to NCMEC. In 2009, PhotoDNA, an image matching software that can detect known CSAM, was donated by our member Microsoft—thereby allowing NCMEC to license it for no cost to entities who want to use its fingerprint-analysis process to identify repeat versions of previously reported images. Simultaneously, widespread use of smartphones and new services entered the marketplace, attracting legions of new users and causing the overall volume of content available online to explode. As a result, the use of existing and newly developed detection tools has significantly increased, as is evidenced by the dramatic growth in the number of CyberTipline reports in recent years.

It is deeply troubling and difficult to fathom the volume of child predation that is detected and reported on an annual basis. It is critically important to remember, however, that each report represents content detected, removed, and reported—creating opportunities for direct law enforcement responses to this important societal issue. And proactive detection means that reported content is often being blocked or removed before it is ever even posted or distributed online. Yet bad actors persist.

Today, IA member companies, alongside governments, civil society, and other stakeholders, continually work to stop bad actors online. IA and its member companies share the goal of eradicating child exploitation online and offline, and our member companies strive to end child exploitation online. They take a variety of actions, including dedicating engineering resources to the development of tools like PhotoDNA and Google's CSAI Match, assisting in the modernization of the Cybertipline through donations of engineering resources or funds, and engaging with law enforcement agencies. Many companies proactively detect and then report instances of CSAM to NCMEC. IA supported the CyberTipline Modernization Act of 2018 to strengthen engagement between NCMEC, the public, and the internet sector and to improve law enforcement's capabilities in the fight to combat child exploitation online and offline.

These are just a fraction of the steps that IA companies take to make the online and offline world a safer place. IA members frequently partner with groups dedicated to ending abuse of vulnerable populations and supporting survivors. Polaris and Thorn are but two examples. IA member companies, where appropriate, may maintain safety resources to educate parents and teen users about online risks and the product features and tools available within the services

[2] Committee on Energy and Commerce Subcommittee on Oversight and Investigations, Making the Internet Safe for Kids: The Roles of ISP's and Social Networking Sites, June 26, 2006.
[3] Public Law 101-401.

to address those risks. In addition, they may point users who are particularly at risk to support organizations that can render real world aid wherever they are located. Many of these resources and programs have been developed in consultation with subject matter experts, including through company-created advisory groups that facilitate broad input or through specific partnerships that target particular challenges.

III. The EARN IT Act Would Create Numerous Problems And Hinder Efforts To Combat CSAM

IA is concerned that the EARN IT Act would burden, discourage, or even prevent, ongoing efforts by internet companies to keep their platforms safe and to identify and remove abusive content. It also would undermine the efforts of law enforcement, and nongovernmental organizations like NCMEC, to hold bad actors to account and combat CSAM online.

1. The bill would be vulnerable to Fourth Amendment challenges that could render evidence from platforms' screening efforts inadmissible, therefore hampering efforts to combat CSAM

Criminal defendants across the United States have filed motions to suppress evidence of child sexual exploitation crimes in the hopes of avoiding conviction.[4] The argument that many of these criminal defendants make is that providers, including IA member companies, who proactively detect CSAM and who report it to NCMEC's CyberTipline, act as "agents of the government" for Fourth Amendment purposes. Under Fourth Amendment jurisprudence, a search performed by an agent of the government is subject to the same requirements as if the government performed the search directly. If a criminal defendant is able to show that the search violated the Fourth Amendment, the exclusionary rule may require that the evidence obtained through the illegal search, and any fruits of the poisonous tree, be excluded at trial.

While these types of motions have been brought by criminal defendants since early use of hashing systems by providers resulted in reports to NCMEC, the number of motions to suppress arguing that providers who proactively detect CSAM are agents of the government swelled following the 2016 Tenth Circuit decision in *U.S. v. Ackerman*.[5] In *Ackerman*, NCMEC was found to be a government actor for Fourth Amendment purposes. This restricts NCMEC's ability to review CSAM reported to it by providers if the providers have not viewed the CSAM themselves. This likewise prevents law enforcement from viewing contents of CSAM reports without appropriate legal authorization.

Defendants' motions to suppress continue to make their way through the courts. Each of these motions represents a criminal defendant accused of crimes against children. If a court determines that a defendant's motion to suppress should be granted on the ground that a provider is an agent of the government and that there was an illegal search, the prosecution will be barred from using not only the CSAM evidence obtained from the provider, but also any

[4] See, for example, *United States v. Reddick*, 900 F.3d 636 (5th Cir. 2018); *United States v. Crawford*, No. 3:18 CR 435 (N.D. Ohio July 16, 2019); *United States v. Tolbert*, Cr. No. 14-3761 JCH (D.N.M. July 7, 2019); *United States v. Miller*, Crim. Action No. 16-47-DLB-CJS (E.D. Ky. June 23, 2017); *State v. Lizotte*, 197 A.3d 362 (Vt. 2018); *State v. Ryan*, 116 N.E.3d 170 (Ohio Ct. App. 2018).

[5] 831 F.3d 1292 (10th Cir. 2016).

other evidence obtained in reliance on that CSAM evidence. Unable to use such evidence, prosecutors will likely be left without sufficient evidence to move forward with the criminal charges, resulting in the defendant going free.

As of now, IA is not aware of a court that has ruled that a provider who proactively detected CSAM and then reported it NCMEC was acting as an agent of the government in doing so. The courts that have ruled on this issue have focused on the voluntary nature of the provider's proactive detection and the independent basis, unrelated to law enforcement objectives, for adopting such a safety measure. These decisions note the requirement of current law that when online service providers gain actual knowledge of apparent CSAM on their services, they must report the facts and circumstances to NCMEC. IA members take this obligation seriously and engage in substantial efforts to report CSAM. Notably, federal law does not *require* providers to take affirmative steps to detect CSAM through monitoring of content, though many internet companies invest significant resources to do so.

If federal law were changed to require that companies search user content for CSAM,[6] or to create a regime in which companies are as a practical matter coerced to do so, then it would be much more likely that courts will deem those companies to be acting as agents of the government when undertaking detection efforts. Under Fourth Amendment principles, this could mean that many defendants' suppression motions that are not being granted under current law would be granted—and many defendants could go free—if the EARN IT Act were passed. It would be difficult to imagine a worse outcome than the routine suppression of critical evidence in CSAM prosecutions—exactly the opposite of what law enforcement seeks to accomplish and totally contrary to the objectives of the companies that now engage in voluntary detection.

The bill states that it should not be interpreted to "require" companies to engage in any particular behavior. But it would nevertheless create a difficult trilemma under which companies would have to choose between (1) following the Commission-determined "best practices" and certifying their adherence; (2) implementing alternative "reasonable measures" in all of the matter areas specified for the Commission's best practices, or (3) doing neither and facing new and uncertain civil liability risks under a reduced "recklessness" standard. Given the serious costs, concerns, and challenges posed by the latter two options, many companies would effectively be coerced into choosing the first option. If one of the "best practices" is for platform operators to engage in affirmative steps to search for CSAM, the company's adherence to it could be said to have resulted from coercion. This would enable defendants to credibly argue that the company undertook its detection activities as an agent for the government, that whatever evidence that the company detected and shared was the result of a search prohibited by the Fourth Amendment, and that both that evidence and whatever else law enforcement learned in reliance on it is unusable in any prosecution.

[6] Because current litigation focuses on proactive detection of CSAM, IA has focused testimony on the impact of a potential best practice related to such activity. IA notes, however, that other potential best practices the Commission could issue may raise similar concerns if they require, for example, gathering evidence that providers would not otherwise collect or retain.

Arguments may be made that courts may avoid this outcome, perhaps by relying on concepts like the third-party doctrine or by theorizing that detection technologies do not perform "searches" for Fourth Amendment purposes. Unfortunately, these are complex legal issues on which existing case law varies, are highly fact dependent inquiries, and require careful consideration by courts. In the wake of the *Ackerman* decision, the questions in this area have already had a profound and detrimental impact. And the EARN IT Act would greatly compound this situation. Defendants would inevitably litigate these issues in virtually every case. Regardless of the eventual outcome, significant investigative and prosecutorial resources that could be devoted to additional CSAM cases would be diverted. Difficult choices would need to be made about which cases to take forward. Providers' CSAM teams, which even under current law are being called upon to travel around the country to testify or otherwise spend time responding to legal process in connection with defendants' suppression motions, would face even greater demands, further diverting key personnel who would otherwise be directly combatting CSAM.

2. The bill would delegate authority to set important standards to an administrative body

The EARN IT Act would delegate important decisions concerning security, privacy, and free speech on the internet—weighty and complex matters that directly impact hundreds of millions of consumers—to an administrative body that would be composed of members who are not elected representatives and that would operate with little transparency. These critical decisions should not be made through an opaque process; rather, they should be made by Congress directly.

It is worrisome that this bill would delegate to a small set of Commission members complex product design decisions that would apply across a highly varied industry. These decisions would not be confined narrowly to CSAM, but rather would impact how lawful content is handled, including through requirements for age gating. This process would have a severe chilling effect on legitimate investment and innovation—if product design decisions can be second guessed by a Commission, every investment decision in a new online service will be clouded with uncertainty.

One important decision that should be addressed by Congress in the first instance is any choice to limit or weaken encryption technology. While the bill does not identify "encryption" as a specific matter that the Commission must address, the Commission is not prevented from addressing it and the bill calls for the Commission to include a privacy, security, or cryptography expert. For these and other reasons, it is widely anticipated that the best practices that might emerge from the Commission would require that companies either weaken, or refrain from deploying, encryption protections for private communications. Limitations on the deployment or strength of encryption would impact a wide range of stakeholders and equities that are not represented on the Commission, as well as topics not within its scope.

Requiring companies to engineer vulnerabilities into their services would make us all less secure. Encryption technology stands between billions of internet users around the globe and innumerable threats—from attacks on sensitive infrastructure, including our highly automated

financial systems, to attempts by repressive governments to censor dissent and violate human rights. Strong encryption is key to protecting our national interests because encryption technology is an essential proactive defense against bad actors.

Giving the government special access to user data—by building in security vulnerabilities or creating the ability to unlock encrypted communications—is impossible without generating opportunities that would be exploited by bad actors. The exponential growth of the internet both deepens and broadens the risks that would be caused by weakening encryption technology. As the internet becomes relevant to more areas of society and the global economy, our exposure to security vulnerabilities expands as well. Foreign and domestic entities have, for decades, targeted private data in hacks aimed at internet companies—a clear threat to our economic and national security. Strong encryption is our best tool for ensuring that the costs of cyberattacks, data breaches, and other types of exposure are low. And encryption can also be a smart strategy to decrease the incentive to engage in hacking. Encryption fundamentally protects the vital interests of our country and its citizens.

3. The bill would be vulnerable to First Amendment challenges

If the EARN IT Act became law, it would be vulnerable to various First Amendment challenges. IA is concerned that such vulnerabilities create legal jeopardy, significant delays, and other costs and impediments that would inevitably slow the achievement of the goals that everyone engaged in the fight against CSAM is trying to attain.

For example, under the unconstitutional conditions doctrine, the government may not deny a benefit—including a discretionary one—based on a person or company's exercise of a constitutional right. When constitutional rights are at stake, the government cannot accomplish indirectly what it is constitutionally prohibited from doing directly. Under the regime envisioned by the EARN IT Act, the government could be viewed as conditioning the receipt of an important government benefit—the long-standing, full protections of Section 230—on companies' waiving certain First Amendment rights to exercise editorial control over what legal user-generated content is available on their services, and to whom it is made available. For instance, were the best practices to require providers to limit access to constitutionally protected speech by age gating content, the law may be held to unconstitutionally conditioned receipt of the benefit of full Section 230 protection on a company's refraining from exercising its First Amendment rights to disseminate protected content.

Additionally, the bill's threat of a carve out from Section 230 protections to induce compliance with government-defined "best practices" could, similar to the Fourth Amendment issues discussed above, convert companies' efforts to remove content into state action, subject to the strict requirements of the First Amendment. By coercing or significantly encouraging a platform to remove certain lawful content, the bill might transform platforms into agents of the government as to that removal. If a company engaged in an aggressive effort to remove CSAM that also sweeped out other non-CSAM content protected by the First Amendment (*e.g.*, family photos, photojournalism, or art), such actions could subject both the government and the companies to arguments that they have imposed unconstitutionally overbroad speech regulation.

The subjects that the bill requires the Commission to address suggest that the best practices might include rules that would be unconstitutional were they compelled. For instance, the best practices must address "age gating systems." But a best practice that would require limiting minors' access to online services could unconstitutionally restrict minors' access to speech protected by the First Amendment or have the effect of unconstitutionally suppressing lawful speech directed to adults. The Supreme Court has consistently held that minors are entitled to a significant degree of First Amendment protection. And it has also held that in attempting to deny minors access to harmful content the government may not unconstitutionally suppress a large quantity of protected speech addressed to and received by adults.

Ultimately, whatever the outcome of such First Amendment challenges would be, it is apparent that the bill would create significant legal issues that could delay or substantially reduce any benefits that might otherwise result from the Commission's work.

IV. Actions That Can Be Taken Today To Combat CSAM

IA is concerned that the EARN IT Act creates unnecessary controversy due to constitutional issues, the spectre of encryption regulation, delegation problems, and concerns about disturbing the wise balance that Congress struck in enacting Section 230. IA member companies do not believe it is necessary to take on these challenging issues in order to pass legislation that would have an immediate positive impact on the fight against CSAM.

The EARN IT Act proposes several immediate, actionable solutions. These include changes to the reporting statute, 18 U.S.C. § 2258A, to improve the content of CyberTipline reports, and to make the reports easier to process. In addition, the bill contains provisions that would allow for greater collaboration among nonprofits and other organizations on their work to combat child exploitation, and protections for content to be analyzed in furtherance of the development of new detection technologies. EARN IT also makes an important update to the U.S. Code by renaming "child pornography" with the more appropriate descriptor "child sexual abuse material." IA supports these provisions but believes more must be done.

For example, the lack of explicit authorization for providers to use CSAM content to develop the next generation of tools that could potentially detect and prevent dissemination of previously unidentified images and victims has slowed the development and deployment of such tools in the United States. IA shares the concern of law enforcement, victim advocates, and policy makers about preventing the misuse of images depicting horrific crimes against children and an understanding that every viewing, even if for a beneficial purpose, re-victimizes that child and is a further violation. However, existing tools for detection of CSAM are highly dependent on matching images that have already been identified as violations, and in response to which there has already been a search for the victim and effort to remove that victim from an abusive situation. While this work needs to continue, IA urges Congress to adopt laws that will create a safe space for the development of tools, such as classifiers and other machine learning techniques, that can identify previously unidentified victims so that they too can be protected.

In addition, there are opportunities to adopt specific legislative provisions now to further support the development of the next wave of detection tools and to aid law enforcement at the

same time. The proposed subjects for the Commission to address include both preservation and retention of material related to CSAM violations, but Commission recommendations will take time and may be subject to constitutional challenges described earlier. The END Child Exploitation Act, which has been introduced in the Senate and the House, would extend the preservation period in the reporting statute from 90 to 180 days to ensure that delays due to the high volume of NCMEC referrals do not result in evidence disappearing before law enforcement is able to request it. It would also allow the voluntary further retention of this material for the development of detection technologies. In addition to being a bicameral and bipartisan effort, that bill has endorsements from NCMEC as well as the Fraternal Order of Police, National Association to Protect Children, Internet Association, Information Technology Industry Council, and Reddit.

The proposed roadmap for the work of the Commission contains ideas on what additional measures could be put in place now or through a streamlined consultation process, such as development of a standard rating and categorization system for CSAM material reported to NCMEC under 18 U.S.C. § 2258A. IA is eager to join with other stakeholders to do the work necessary to determine the most needed changes and the best way for those changes to be achieved.

IA also supports the collection of better data about the current scale of the problem, the collective actions being taken, and the opportunities for improvement. Earlier this month, a letter signed by Senator Maggie Hassan (D-NH), Senator Marsha Blackburn (R-TN) and Representatives Annie Kuster (D-NH) and Anthony Gonzalez (R-OH) was sent to the Government Accountability Office (GAO) urging a review of the federal government's efforts to combat on child exploitation. GAO performed a similar review in 2011 as required by the PROTECT Our Children Act of 2008. The letter requests that GAO undertake a thorough examination of the scale of the problem, the efforts that have been undertaken to fulfill the mandates of the PROTECT Our Children Act, and the actions and cooperation among the key stakeholders in addressing this problem, including federal, state and local law enforcement, industry, victim advocates, NCMEC and many others. IA views this type of thorough review as critical to shaping appropriate government responses to the current situation.

Among issues a review could consider is to what extent state and local law enforcement, who are on the front lines of this fight, and NCMEC, which also plays a key role, are appropriately resourced given the scale of reporting, technological advances, and adjustments made in the wake of the *Ackerman* case. IA supports increased appropriations to law enforcement and NCMEC to ensure adequate resources are available to meet this challenge. Importantly, funding should also ensure adequate resources for victim's assistance, compensation, and recovery.

This Committee is in a position not only to request, but to require, that the necessary review be performed and that the data that are needed to understand and monitor this problem are collected and published on an ongoing basis. Government reporting on statistics related to specific criminal offenses and law enforcement investigations and prosecutions exists currently. A review of the Administrative Office of the U.S. Courts data show that for the 12-month period ending December 31, 2018 that 660 criminal defendants were prosecuted in

federal district courts for sexual abuse offenses against minors.[7] There is a critical need to understand how this statistic relates to the volume of reports received by NCMEC in the same year, and the results of those reports. It would also be helpful, in order to better understand the scale of the problem and the challenges it creates for analysis, investigation, and prosecution of CSAM violations, to have more detailed data available on provider CyberTipline reports. For instance, it would be beneficial to know how many reports are forwarded internationally as it appears that in recent years over 90 percent of reports were related to individuals uploading CSAM from outside the United States.[8] It would also be helpful to know how many of the reports NCMEC receives represent content that was detected and blocked before ever being posted on or distributed through a platform. And it would be helpful to know how many unique violations are represented within the total report numbers. For example, how often are multiple reports generated on the same offender because of the large volume of content they seek to distribute being split into individual reports?

Several IA member companies have started self-reporting data on CSAM identification and removal. This builds on established practices at those companies to provide transparency for their users, the public, government, and public interest organizations on their policies, how they are enforced, and the prevalence of the offending content on their networks. As these reports together represent a vast majority of the reports sent to the CyberTipline, they help shed light on provider efforts. For example, the reports are helpful for understanding what proportion of CSAM content detected and removed from provider services is detected proactively or through automated means versus through user or third-party reports. IA was pleased that transparency was raised as an important part of the discussion on terms of service enforcement at DOJ's recent roundtable on Section 230.

Additional transparency on the full lifecycle of CSAM—beginning with the abuse itself, to the creation and distribution of the evidence of the abuse, its detection, investigation and prosecution, to the measures taken to support recovery for victims and prevent recidivism by the perpetrators—would fuel new and creative solutions to a problem our society has struggled with for too long.

V. Section 230 Has Important Benefits And Allows Punishment of Bad Actors

Section 230 empowers internet companies to identify and remove CSAM and other illegal or harmful material. Section 230 was enacted in response to a court decision that exposed internet companies to liability based on their efforts to block objectionable third-party content. Congress feared that if internet companies could be liable due to their monitoring and moderating objectionable content, they would be discouraged from performing even basic safety removal to avoid incurring liability. Section 230 removes this disincentive to self-regulation by shielding service providers from claims that would hold them liable due to their attempts to moderate certain content. As a consequence, Section 230 has effectively

[7] Administrative Office of the U.S. Courts, Statistical Table: Criminal Defendants Terminated, by Type of Disposition and Offense, December 31, 2018 (available at: https://www.uscourts.gov/statistics/table/d-4/statistical-tables-federal-judiciary/2018/12/31).
[8] https://docs.house.gov/meetings/JU/JU08/20170316/105712/HHRG-115-JU08-Wstate-ShehenJ-20170316.pdf (Mar. 16, 2017).

encouraged service providers to engage in responsible self-regulation, including in efforts to combat CSAM.

Passed as part of the Communications Decency Act in 1996, Section 230 created two key legal principles. First, internet companies that provide platforms for user-generated content generally cannot be held liable based on their users' content, whether it consists of blogs, social media posts, photos, professional or dating profiles, product and travel reviews, job openings, or apartments for rent. And second, online services—whether newspapers with comment sections, employers, universities, neighbors who run listservs in our communities, volunteers who run soccer leagues, bloggers, churches, labor unions, or anyone else that may offer a space for online communications—can moderate and delete harmful or illegal content posted on their platform without being held liable based on their actions to block or remove that content. Most online platforms—and all of IA's members—have robust codes of conduct, and Section 230 allows the platforms to enforce them without fear of litigation and liability.

Without Section 230's protection, internet companies would be left with a strong disincentive to monitor and moderate content. Section 230 removes this disincentive to self-regulate, creating essential breathing space for internet companies to adopt policies and deploy technologies to identify and combat objectionable or unlawful content—or to develop other innovative solutions to address such content.

Section 230 embodies Congress's thoughtful strategy to remove this roadblock to self-regulation. Generally, Section 230 protects internet companies, subject to certain exceptions, from lawsuits that seek to hold them liable for user-generated content or their efforts to remove objectionable material. Under Section 230, it is the originators of unlawful content, not the platforms who merely carry it, who are appropriately subject to liability. By creating this protection, Congress has successfully encouraged internet companies to engage in self-regulation as evidenced by, among numerous other examples, companies' very substantial and proactive efforts to combat CSAM. And this protection is precisely what has enabled companies to pursue proactive efforts to identify, block, remove, and report CSAM.

Section 230 is also essential to fostering an environment conducive to startup internet companies and new market entrants. Without Section 230, small and medium-sized businesses would be exposed to, but unable to quickly end, litigation arising from their carriage of third-party content. While some internet companies are no longer upstarts, IA represents more than 40 internet industry companies of which the vast majority are unlikely to be considered "titans." The technology industry still features a vibrant pipeline of startups that fuels continued innovation. Weakening Section 230 by imposing additional exposure to litigation and potential liability would be a burden felt disproportionately by new market entrants and small and medium-sized companies.

A number of misconceptions about Section 230 cloud the important discussion regarding efforts to combat CSAM. Section 230 does not grant immunity to those who themselves create, develop, or distribute unlawful content, including bad actors who violate child exploitation laws. And Section 230 expressly provides that it does not restrict the enforcement of federal criminal law, including laws targeting child exploitation against providers. IA supports efforts to enforce these criminal laws against those who illegally create, develop, or distribute CSAM

and urges Congress to put more resources behind these efforts. The Department of Justice's press releases announce numerous successes in prosecutions against online services for criminal activities, such as advertising of CSAM. As just one example, the DOJ announced last month that a defendant pleaded guilty to conspiring to advertise CSAM by operating an anonymous web service.[9]

Conclusion

The victims of CSAM should not have to wait for the proposed Commission to do its work, Congress to approve best practices, and constitutional challenges to work their way through the courts for help. On an issue that attracts strong support from a vast array of interests, there should be an ability to move forward to implement new authorities to support the fight against CSAM based on consensus. IA and its member companies look forward to working with the bill sponsors, this Committee, other lawmakers and stakeholders to pass measures that can be implemented now to address this vital concern.

9 https://www.justice.gov/opa/pr/dark-web-child-pornography-facilitator-pleads-guilty-conspiracy-advertise-child-pornography (Feb. 6, 2020).