Prepared Written Testimony

Mary Graw Leary,

Professor of Law, The Catholic University of America

Children's Safety in the Digital Era: Strengthening Protections and Addressing Legal Gaps

Senate Judiciary Committee

February 19, 2025

2026 Dirksen Senate Office Building

Introduction

Thank you for the invitation to appear before you today to discuss children's safety in the digital era and the gaps in the law to protect them. My name is Mary Graw Leary and I am a Professor of Law at the Catholic University of America, Columbus School of Law. As an academic, my scholarship focuses on the exploitation of vulnerable people, especially women and girls; crime victim rights; and the intersection of criminal law and technology.[1] From that perspective I have written extensively about online exploitation, the role the technology industry plays in facilitating it, and §230 of the Communications Decency Act. I have studied the history and intent of § 230 of the Communications Decency Act and several forms of exploitation including, but not limited to child sexual abuse material (CSAM), human trafficking, and nonconsensual sexual material. In this work I have observed and studied the forms of exploitation facing children on a case by case level, but also on a national level, seeing them become more expansive and pernicious.

As I begin my comments, I approach the title of this hearing as a question: are children safe in the digital era? The answer is an emphatic "no." The title of the hearing is insightful as to the reasons why: the law has several significant legal gaps.

The reasons for this are many. But I will focus much of my comments on the distortion of §230 of the Communications Decency Act which is the direct cause of an ecosystem that not only fails to protect children but incentivizes the tech industry to put them at risk and cause harm with impunity.

To adequately discuss §230 of the Communications Decency Act, two principles must frame our discussion. First, the myths surrounding the history of the purpose of §230 of the Communications Decency Act must be dispelled as the law is properly understood as a *law emerging out of a landscape of child protection*, not one seeking solely internet freedom. The second framing principle is that at the time of the debate and creation of this law, it can be consider an experiment – an experiment its proponents argued would protect children and families from exploitation and indecent content. With this framing in mind, we must then examine the results and effects of this experiment regarding exploitation and indecent content. By "result" I intend to discuss what happened to the protective law since its passage in 1996 and the campaign of the tech industry to distort it from a law of limited protection to one of de facto near absolute immunity. By "effect," I intend to discuss the massive harms this distortion causes children.

[1] E.g., **The Indecency and Injustice of the Communications Decency Act,** *Harvard Journal of Law and Public Policy*, Vol. 41, No. 2 (2018); **History Repeats Itself: The New Faces Behind Sex Trafficking Are More Familiar Than You Think,** *Emory Law Journal Online*, Vol. 68 (2019); **The Third Dimension of Victimization**, *Ohio State Journal of Criminal Law*, Vol. 13, No.1 (2016); **The Digital Nexus of Commercial Exploitation of Children and Adolescents in the United States: From the Streets to Cyberspace,** *Sexual Development, The Digital Revolution, and the Law*, Oxford University Press (Co-Authored) (2014).

Here, it is apparent that the threats facing children in the digital era are profound both in their volume and severity, and that these effects did not occur by accident. Rather, they are a direct result of the tech industry actively distorting the intent of §230 of the Communications Decency Act in courtrooms across the country to transform it from a law intended to incentivize protection to one that incentivizes harmful actions by providing de facto near absolute immunity for them.

Therefore, with these framing principles and examination of the harm, there is one conclusion. This experiment of a distorted §230 of the Communications Decency Act has failed. I suggest Congress must act to remedy this and offer some principles to consider including the need to amend §230 of the Communications Decency Act and return it to its original purpose: limited immunity to protect children, not de facto near absolute immunity to harm them.

I. Principle One: Section 230 of the Communications Decency Act Emerged from a Child Protection Landscape

Section 230 of the Communications Decency Act must first be understood as a law that emerged out of a landscape of child protection. Although the tech industry and its surrogates attempt to frame it as a stand-alone provision solely to protect the Internet, that is incorrect. While that is not to say it is a "child protection statute;" it is not as it addressed multiple concerns. However, the backdrop of the discussion was protection and the structure, history and text, of the legislation reflect §230 of the Communications Decency Act emerged from a landscape of child protection.

A. The Structure of §230 of the Communications Decency Act Demonstrates It Emerged From a Child Protection Landscape

This legislation is often referred to as simply "§230." That is a mistake as doing so can be misleading – divorcing it from its purpose. Its title and location in the U.S. Code make clear it is legislation emerging from a child protection context. The full title of § 230 is *Protection for Private Blocking and Screening of Offensive Material*. By this very title Congress was clear as to the protection intended: **for** blocking and screening of offensive material – not protection for disseminating harmful material. This is abundantly clear with its placement within the Communications *Decency* Act (CDA) which became part of the Telecommunications Act of 1996. As it updated the telecommunications legal infrastructure, Congress in its wisdom recognized that the potential for exploitive material and child abuse occurring on this new medium - without the old medium's guardrails - was high. Therefore, as part of the Telecommunications Act, Congress directly addressed that and included the CDA within this law. If that were not clear enough, it placed the Communications Decency Act within the *Obscenity and Violence* title and the *Obscene, Harassing,* and *Wrongful Utilization of Telecommunications* subtitle. All these

structural efforts reflect this history and this legislation was not a stand-alone bill designed for broad immunity but one specifically targeting indecent material and exploitation.[2]

B. Legislative History and Contemporary Coverage of the Creation of §230 of the Communications Decency Act Demonstrate Its Emergence From a Child Protection Landscape

In 1996 Congress faced regulatory questions around "new" mediums such as cable television, digital communication, and a nascent dial up World Wide Web. It embarked on an effort to update the outdated 60 year old Communications Act of 1934. At that time Congress did not even imagine today's Internet. In 1996 only 20% of users went online every day and the average American spent less than 30 minutes a month exploring the Internet, dial up was the main form of connection, and users numbered less than 45 million people worldwide.[3] Social media was not yet the norm. Twitter, Facebook, Snap, Pornhub, Grindr, or TikTok did not exist. Regarding sexual exploitation material, the Supreme Court stated that "users seldom encounter such content accidentally. . . . 'Almost all sexually explicit images are preceded by warnings as to the content.'"[4]

To its credit, however, many members of Congress were aware of the risks of platforms expanding explicit and harmful material, CSAM (then described at child pornography), cyberstalking, and adult sexual offenders gaining unprecedented access to children.[5] To address these concerns, the Senate proposed a bipartisan and revised Communications Decency Act as part of the Telecommunication Act to protect children and families from indecent material.[6] It is important to note that even those senators who opposed the CDA on other grounds, explicitly recognized the CDA was designed from a protective framework and endorsed the goal to "protect children from obscene and indecent material."[7] Thus, this effort to limit the spread of indecent material and protect children was shared by many and the Telecommunications Bill passed the Senate 81-18.

In the House of Representatives, two Congressmen responded to both the CDA approach to limit this material at the point of distribution and a New York state trial court defamation decision *Stratton*

---

[2] Telecommunications Act of 1996, Pub. L. No. 104, 110 Stat. 56 (1996); 47 U.S.C. 230(b)(1),(2).
[3] E.g., Reno v. A.C.L.U, 521 U.S. 844, 850 (1997); Farhad Manjoo, Jurassic Web, **Slate** (Feb. 24, 2009, 5:33 PM) .
[4] Reno, 521 U.S. at 853 (quoting ACLU v. Reno, 929 F. Supp. 824, 844 (E.D. Pa. 1996)).
[5] 141 Cong.Rec.S1954 (daily ed. June 9, 1995).
[6] 141 Cong. Rec. S8088 (daily ed. June 9, 1997) (comments of Sen. Exon)("The fundamental purpose of the Communications Decency act is to provide much needed protection for children."); *see also* 141 Cong. Rec. S8089 ("The heart and soul of the Communications Decency Act are its protections for families and children.").
[7] E.g., 141 Cong. Rec. S8331 (daily ed. June 14, 1995) (comments of Sen. Leahy)(endorsing the need to "keep hardcore pornography away from our children," imprison child pornographers, but also have a functioning Internet.).

Oakmont v. Prodigy Services Co.[8] Stratton Oakmont sued Prodigy for defamation regarding an anonymous post on its financial services bulletin board accusing Stratton Oakmont of fraudulent practices. In contrast to precedent and reality,[9] this state court found Prodigy responsible for that third party content in part because of Prodigy's active screening out of inappropriate material.[10] The court considered Prodigy a publisher of the information under state law because "it voluntarily deleted some messages . . . and was therefore legally responsible for the content of defamatory messages that it failed to delete."[11] Counterintuitively, the trial court held Prodigy responsible for the post because it attempted to monitor its board while in previous cases similarly situated platforms were not considered publishers of such third party content.[12] Notwithstanding that this was a singular state level opinion, two members of the House were concerned about the implication of that case on the CDA's framework of stopping material at the point of distribution. Within the context of the child protection debate that the CDA began, these congressmen proposed the Internet Freedom and *Family Empowerment Act* of 1995 (IFFE)(emphasis added). As the name suggests, this bill was concerned with both internet issues but also in *protecting families*, not in protecting platforms. The debate was never *whether* to limit indecent material and shield families, but *how* to do so effectively.

Therefore, among other goals, IFFE did not want to disincentivize a company from monitoring its platforms for improper third party content by having them face liability for doing so.[13] A backdrop of the discussion with this bill was legislating the most effective method to limit indecent and harmful material. The IFFE approach was attached to the House version of the Telecommunications bill.

The Telecommunications bills went into committee negotiations with two different versions on how to address indecent material and protect children. The first from the Senate, the CDA, acknowledged

---

[8] No. 31063/94, 1995 WL 323710, *2 (N.Y. Sup. Ct. 1995); *contra, Cubby, Inc. v. Compuserve, Inc.*, 776 F.Supp. 135 (SDNY) (Dismissing defamation action against defendant who sold access to library of news publications because defendant was a mere distributor and not a publisher.)

[9] Ironically, the leadership of Stratton Oakmont pled guilty to stock manipulation occurring during this time. Edward Wyatt, Stratton Oakmont Executives Admit to Stock Manipulation, New York Times (Sept. 24, 1995).

[10] No. 31063/94, 1995 WL 323710, *2 (N.Y. Sup. Ct. 1995); *contra, Cubby, Inc. v. Compuserve, Inc.*, 776 F.Supp. 135 (SDNY) (Dismissing defamation action against defendant who sold access to library of news publications because defendant was a mere distributor and not a publisher.)

[11] Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157, 1163 (9th Cir. 2008) (citing Stratton Oakmont v. Prodigy Servs. Co., 1995 WL 323710, *4 (Sup. Ct. May 24, 1995)).

[12] Stratton Oakmont v. Prodigy Servs. Co., 1995 WL 323710 (Sup. Ct. May 24, 1995); *see also* Doe v. AOL, 783 So. 2d 1010, 104 (2001) (citing Steven M. Cordero, Comment, Domnum Absque Injuria, Zeran v. AOL: Cyberspace Defamation Law, 9 FORDHAM INTELL. PROP., MEDIA AND ENT. L.J. 775 (1999).

[13] Christopher Cox, *The Origins and Original Intent of Section 230 of the Communications Decency Act*, UNIV. RICH. J. L. AND TECH., 64 (2020) (Its sponsor has also argued it was important to respond to Stratton Oakmont because "common law extended no protections to platforms that moderate user content."); Stratton Oakmont v. Prodigy Servs. Co., 1995 WL 323710, *1 (Sup. Ct. May 24, 1995).

the value of the Internet[14] but also prioritized shielding children and families from explicit content and ensuring it would not facilitate child abuse and exploitation. The IFFE, while respecting the concerns of the CDA, sought, *inter alia,* to incentivize platforms to monitor their sites promising this would protect children and families. It is critical to understand the text of Section 230 of the Communications Decency Act of today emerged from this landscape of protection.

Following months of negotiation, the final Telecommunications Act of 1996 struck parts of IFFE but embraced both approaches to protecting children by including parts of the text of the IFFE within the CDA under Section 230. By placing the protective language of IFFE *into* §230 of the CDA, this statute must be read as being anchored in shielding families from indecent materials by incentivizing platforms to do just that.

Although the technology industry, their surrogates, and even authors of the IFFE at times try to divorce Section 230 from these roots, that is how it was situated within the law as it emerged from Conference and how it was passed by Congress. Contemporary Congressional debate around the legislation reflects that Title V- which housed this small language from the IFFE concepts as a component of the CDA – reflects this child protection landscape.[15] Obviously, the 107 pages of the Telecommunication Act of 1996 had many goals.[16] But Congress made clear by including §230 of the CDA within the Obscenity and Violence Title that this Section possesses child protection elements.[17] Chief Judge Katzmann described this history of Section 230 by noting that,

---

[14]141 CONG. REC. S8089 (daily ed. June 9, 1995) (comments Sen. Exon) ("The computer is a wonderful device for arranging, storing, and making it relatively easy for anyone to call up information or pictures on any subject. That is part of the beauty of the Internet system.").

[15] When the Senate was actually debating the Conference Report, one Senator noted that "the Internet indecency provisions have met with the barest of resistance in this Chamber.");142 Cong. Rec. 1993, 2036 (comments of Sen. Feingold).

[16]142 CONG. REC. 1993, 2041 (comments of Sen. Exon) ("Concurrent with our efforts to make the Internet and other computer services safe for families and children, this bill includes legislation which will help turn the information revolution to the benefit of all Americans, but especially America's children."); "a needed step in protecting children from child molesters and unscrupulous porn merchants," noting the need for federal legislation in this area, not just new technologies. 142 CONG. REC. 1993, 2041.

[17] *E.g.,* 142 CONG. REC. 1993, 2013 (comments of Sen. Stevens) (noting this is not a deregulation bill); *see also, id.* at 2030 (comments of Sen. Coats) ("Perhaps most importantly this bill will help protect children from computer pornography which today is readily accessible on the internet."). One Senator noted that "the Conference Report contains strong protections for America's children." 142 Cong. Rec. 1993, 2030 (comments of Sen. Holmes); 142 Cong. Rec. 1993, 2030 (comments of Sen. Coats)(noting the linkage between the bill and protecting children from not only pornography but "images and text dealing with the sexual abuse of children."). Although there were opponents to the bills, the framing of its protective purpose was not in dispute. *E.g.,* 142 Cong. Rec. 1993, 2015 (comments of Sen. Leahy)(acknowledging that "[a]ll of us 100 members of the U.S. Senate oppose the idea of child pornography," but expressing constitutional concerns about two provisions of the CDA outside §230); 142 Cong. Rec. 1993, 2035 (comments of Sen. Feingold)(discussing the legislation as redundant to current federal laws regarding child abuse, stating that "much of what the proponents of this legislation wish to banish from cyberspace

> [o]f the myriad of issues the emerging Internet implicated, Congress tackled only one: the ease with which the Internet delivers indecent and offensive material, especially to minors….The Conference Committee had two alternative versions for countering the spread of indecent online material to minors. The Committee chose not to choose. Congress instead adopted both amendments as part of the final Communications Decency Act.[18]

Congress viewed §230 of the Communications Decency Act as a tool in the toolbox of combatting indecent material and protecting children, as well as protecting platforms from liability for efforts to do so themselves.

C. The Text Itself Demonstrates §230 of the Communications Decency Act Emerged From a Child Protection Landscape

Although it has since been distorted by the tech industry, the plain language of §230 of the Communications Decency Act explicitly underscores this child protection backdrop. An example is Congress's naming of the section "Protection for Private Blocking and Screening of Offensive Material." The word "protection" is important but more important is the explicit statement for what a platform would receive protection: blocking and screening of offensive material not for failing to do so or for facilitating such material. Notably, the word "immunity" is absent. From this text.

Congress included five statements of the policy of the United States. Three policies speak to the protective intentions behind the bill.[19] Among those, the statute explicitly states that it is the policy of the United States to "ensure vigorous enforcement of Federal criminal laws to deter and punish *trafficking in obscenity, stalking, and harassment by means of [a] computer*"--the very concerns mentioned in the CDA debates. The inclusion of these policies, combined with the text of the provision that explicitly states the statute should have no effect on enforcement of obscenity and child exploitation federal criminal law, reflect the climate from which § 230 came: a discussion about the best methods to protect children from explicit material and exploitation.

Critical to the supporters of the IFFE, § 230 of the Communications Decency Act includes language providing what was intended to be limited protection for platforms. As the title of §230 of the Communications Decency Act suggests, the protection includes protection from civil liability for "Good Samaritan" blocking or screening of offensive material made in good faith. Congress explained "offensive material" is "material that the provider or user considers to be obscene, lewd, lascivious,

---

is already subject to criminal penalties – obscenity, child pornography, and child exploitation via computer networks are already criminal acts.") Those who opposed the CDA did so on other constitutional grounds unrelated to §230 of the CDA which were resolved in Reno v. ACLU, 521 U.S. 844, 874 (1997).

[18]Force v. Facebook, 934 F.3d 53 (2d Cir. 2019) (Katzmann, CJ dissenting). Chief Justice Katzmann also rejected the argument that Section 230 had nothing to do with the CDA and observed that its placement within the CDA was not coincidence.

[19] 47 U.S.C. §230(b).

filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected."[20]

Not only does this provision reflect the clear intent of Congress to offer limited protection to platforms, it confirms the protection from civil liability is related to child and family protection. The other protection from liability is located in §230(c)(1) and describes not treating platforms as publishers. "Looking at the text…§230(c)(1) does not 'declare a general immunity from liability deriving from third-party content.' Indeed, §230(c)(1) 'does not mention 'immunity' or any synonym.'"[21] Rather, ICSs were protected only from publisher liability--not distributor liability. "*Stratton Oakmont*'s rule created a perverse incentive not to moderate any offensive content, and Congress was concerned. So, in 1996, Congress enacted 47 U.S.C. § 230 [and] … was meant to bring traditional "distributor" immunity online."[22] To read it otherwise is manufactured. As Justice Thomas noted, "[i]t is odd to hold, as courts have, that Congress implicitly eliminated distributor liability in the very Act in which Congress explicitly imposed it."[23]

Furthermore, the legislation explicitly states that it will not affect the enforcement of any criminal statute, but also specifically mentions not impacting laws relating to obscenity and the sexual exploitation of children.[24] This text reflects many priorities, and explicitly includes child protection. The Report's discussion concerning the CDA and IFFE's goals of developing the most effective methods to protect children supports the plain language understanding of the text. The Conference Report states:

> This section [§ 230] provides "Good Samaritan" protections from civil liability for providers or users of an interactive computer service for actions to restrict or to enable restriction of access to objectionable online material. . . . The conferees believe that such decisions [similar to Stratton Oakmont] create serious obstacles to the important federal policy of empowering parents to determine the content of communications their children receive through interactive computer services.[25]

Therefore, as a framing principle, §230 of the Communications Decency Act must be understood not as a stand-alone bill asserting broad immunity, but as a narrow bill (albeit with multiple goals)

---

[20] 47 U.S.C. §230(c)(2).
[21] Calise v. Meta Platforms, Inc, 103 F.4th 732, 740 (9th Cir. 2024)(quoting *Barnes v. Yahoo!, Inc.*, 570 F.3d 1096, 1100 (9th Cir. 2009) and Chi. Lawyers' Comm for Civ. Rts. Under Law, Inc. v. Craigslist, 519 F.3d 666, 669 (7th Cir. 2008).
[22] Calise, 103 F.4th at 739. See also [22] Malwarebytes, Inc. v. Enigma Software Grp. USA, LLC, 141 S. Ct. 13, 14-15 (2020) (mem.).
[23] Malwarebytes, Inc. v. Enigma Software Grp. USA, LLC, 141 S. Ct. 13, 14-15 (2020) (mem.).
[24] 47 U.S.C. §230(e).
[25] Telecommunications Act of 1996, S. Rep. No. 104-230, at 194 (1996) (emphasis added).

emerging out of a landscape of protection from child exploitation and harm. This is supported by the structure, history, and text of the legislation.

II. Principle Two: The IFFE Provisions Were Effectively An Experiment Based Upon the Promise That if Included They Would Be the Strongest Way to Protect Children and Families

The second framing principle is that the current text of the §230 of the Communications Decency Act was offered as an experiment and that has failed. Whether analyzing the forces behind the IFFE or the support for the final version of §230 of the Communications Decency Act it is essential to understand the basic promise proponents made in including §230(c)(1). They promised that these provisions would be the most effective way to protect children and shield explicit conduct because read together §230(c)(1) and (c)(2) would incentivize platforms to monitor and prevent this content. However, the way in which §230 of the Communications Decency Act has been distorted, it has not.

That is to say that the final text of the §230 of the Communications Decency Act was Congress accepting the invitation of the proponents of the IFFE and the tech industry to experiment that (c)(1) would be protective. Critically, companies argued that such an approach encouraged, indeed promised, that tech companies would produce workable technologies that would allow parents and users to filter out such material.[26]

By incorporating parts of the IFFE into the CDA, Congress prohibited both the illegal transmission of such material, but also accepted the industry's promise that it would utilize the incentive to develop parental controls and filters and provide them to the public.[27] Additionally, this was the vision of IFFE proponents who argued that both federal law and technological solutions were needed to protect children.[28] This was the experiment: a twofold approach with narrow limited liability for efforts to protect children would lead to a safe internet. Although that technology did not exist, the tech industry happily promised it would develop it and it would become more sophisticated and easily available to parents.[29]

---

[26] Steve Lohr, Conservatives Split on How to Regulate the Internet, **N. Y. Times**, Nov. 9, 1995, at D4 ("Both camps agree on the need to protect children from offensive material on computer networks. But the methods they advocate represent two divergent views on how to regulate the fast-growing medium.").

[27] Nicolas Conlon, Freedom to Filter Versus User Control: Limiting the Scope of § 230(C)(2) Immunity, 2014 **Univ. Ill. J. L. Tech. & Pol'y** 105, 115.

[28] See Kara Swisher, Ban on On-Line Smut Opposed, **Wash. Post**, July 18, 1995, at D3 (describing how the tech industry and law makers worked on a compromise, including the consideration of several proposals, such as replacing the term "indecent" to "harmful to minors" and implementing credit card verification as a means of restricting access).

[29] Robert Corn-Revere, New Age Comstockery, 4 **Comm. L. Conspectus** 173 (1996).

Contemporary news accounts demonstrate the tech companies' false promises about the ability of what would become § 230 to protect children.[30] These representations were not inconsequential but a component of an intensive lobbying effort to embrace this experiment."[31] The Washington Post described how "[o]n-line companies, software makers and civil liberties groups came to Capitol Hill yesterday to make their case that the on-line world can be made safe for children without government intervention."[32] The result of this effort was characterized as one in which some "reject[ed] promises from the on-line industry that companies like [AOL] and Netscape Communications Corp. would give parents tools to screen offensive material if they could be sure such actions wouldn't make them liable for any message sent by any subscriber."[33] The rejection of this promise was prophetic. The Department of Justice studied the effects of § 230, concluding that this "expansive statutory interpretation, combined with technological developments, has reduced the incentives of online platforms to address illicit activity on their services."[34] Moreover, the public has not seen the type of screening or parental controls suggested. While the tech industry argues that it does provide controls,[35] a common chorus is that they are neither effective, nor readily accessible.[36] That is exactly the opposite of what the §230 proponents promised.

Congress intended this statute to provide limited protection to platforms based on their representation that such immunity would empower platforms to protect children and families. This experiment has failed because the tech industry has replaced limited liability with de facto near absolute immunity.[37] As the Ninth Circuit noted, "when an internet company has an economic incentive to permit

---

[30] The Washington Post reported that tech companies promised to provide and utilize technology to filter out such material. Kara Swisher & Elizabeth Corcoran, Gingrich Condemns On-Line Decency Act, **Wash. Post**, June 22, 1995, at D8.

[31]The New York Times reported that "Interactive Services Association, a trade group for the on-line industry that supports the Cox-Wyden Amendment," demonstrated for the staff members of the conferees on the telecom bill "software that can filter out material deemed objectionable. Lohr, supra note 26.

[32] *E.g.*, Swisher, supra note 28, at D3.

[33] Daniel Pearl, Compromise Sought on Curbs for the Internet: On-Line Service Firms Seek to Check Harsh Rules on Controlling Content, **Wall St. J.**, Dec. 4, 1995, at B8.

[34] *Department of Justice's Review of Section 230 of the Communication Decency Act Of 1996*, Dep't. of Just. Archives, https://www.justice.gov/archives/ag/department-justice-s-review-section-230-communications-decency-act-1996.

[35] *E.g.*, Our Tools, Features and Resources to Help Support Teens and Parents, **Meta**, https://www.meta.com/help/policies/safety/tools-support-teens-parents/ [https://perma.cc/2AFG-ZJ6U] (Dec. 2024).

[36] *E.g.*, Brian Fung & Clare Duffy, Kids Aren't Safe on Social Media, Lawmakers Say. Tech CEOs Are Back in DC to Pledge (Again) that They'll Handle It, **CNN Bus.** (Jan. 29, 2024, 6:42 PM), https://www.cnn.com/2024/01/29/tech/big-tech-ceos-youth-safety-senate-testimony/index.html [https://perma.cc/66J3-M4QC]; Tatum Hunter, Instagram's New Teen Safety Features Still Fall Short, Critics Say, **Wash. Post** Jan. 10, 2024; IWF, Meta Failing to Stop Spread of Sexual Abuse Imagery In the Wake of the Huw Edwards Scandal (Aug. 16, 2024).

[37] The OSCE studied global laws and that a system of allowing self-regulation has largely failed. OSCE, Policy Responses to Technology-Facilitated Trafficking in Human Beings (2022).

unlawful content to be posted by third parties, it seems to encourage the opposite [of self-regulation] – willful blindness."[38]

III. The Result of this Failed Experiment Is De Facto Near Absolute Immunity

As will be discussed in Section IV, that §230 of the Communications Act failed to protect children and families from exploitation and indecent content is beyond dispute. Statistics from NCMEC, Interpol, Internet Watch and others all underscore the harms of exploitive content delivered to children on tech's platforms.[39] Had the language of §230 of the Communications Decency Act been adhered to, it is possible that the concept of limited protection from civil liability for Good Samaritans would have provided the incentive to create a protective regime. But it did not. In large part because after making such promises, those tech companies embarked on an effort to expand this immunity. They did so by advocating in courtrooms across America for an interpretation of § 230 providing much broader immunity than legislators intended or the text reflected, and caused its expansion far beyond its original purpose.

This began with the very first published opinion, *Zeran v. America Online*.[40] In this defamation case, the Fourth Circuit focused on the policies of §230 of the Communications Decency Act relating to limited regulation, but ignored the numerous other policies regarding protections from indecent material.[41] Its language characterizing §230 of the Communication Decency Act as "broad" took on a life of its own in subsequent cases. Recently, however, more judges have been calling for a return to the text and for Congress acknowledged to correct it.[42]

With tech companies and their surrogates throughout the country seizing on this language, many courts have accepted this early characterization as true, and, instead of quoting from the text of the legislation, quoted heavily from *Zeran*, notwithstanding the textual and historical record. These include

---

[38] Calise, 103 F.4th at 747 (Nelson, J. concurring).

[39] Interpol & ECPAT Int'l, **Towards a Global Indicator on Unidentified Victims in Child Sexual Exploitation Material: Summary Report** 1 (2018); Internet Watch Found., **WF Annual Report 2023 #Behind the Screens**, (2023); Department of Justice Press Release, **FBI and Partners Issue National Public Safety Alert on Sextortion Schemes** (Jan. 19, 2023); NCMEC**, 2023 Cybertipline Report** (2024).

[40] Zeran v. Am. Online, Inc., 129 F.3d 327 (4th Cir. 1997).

[41] Zeran v. Am. Online, Inc., 129 F.3d 327, 330 (4th Cir. 1997). At one point the Fourth Circuit did acknowledge that "Section 230 was enacted, ***in part,*** to maintain the robust nature of Internet communication and, accordingly, to keep government interference in the medium to a minimum." Id. However, it never explained the other purposes of §230 which demonstrate the very limited immunity and that qualifier has largely been ignored.

[42] *E.g.*, Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157, 1163 (9th Cir. 2008); Jane Doe #1 v. MG Freesites, Ltd., No. 7:21-cv-00220-LSC, 2022 U.S. Dist. LEXIS 23199 (N.D. Ala Feb. 9, 2022); Doe v. Am. Online, 783 So. 2d 1010, 1019 (Fla. 2001) (Lewis, J. in dissent); Calise v. Meta Platforms, Inc, 103 F.4th 732, 740 (9th Cir. 2024); Doe v. Snap, Inc., 88 F.4th 1069, 1070 (5th Cir. 2023) (per curiam) (Elrod, J., dissenting from denial of reh'g en banc) (describing the interpretation as "sweeping immunity for social media companies that the text cannot possibly bear.")

an early case finding immunity for a civil allegation that a platform distributed CSAM, allowed advertisements for CSAM, and a failed to respond to notification that its services were being utilized to distribute obscene material. [43] In Doe v. America Online, the dissent was clear:

> Contrary to the majority's view, however, the carefully crafted statute at issue, undergirded by a clear legislative history, does not reflect an intent to totally exonerate and insulate an ISP from responsibility where, as here, it is alleged that an ISP has acted as a knowing distributor of material leading to the purchase, sale, expansion and advancement of child pornography . . . .[44]

The concerns of the dissent in that case prophetically forewarned this would create "carte blanche immunity for wrongful conduct plainly not intended by Congress."[45]

This concerted effort by tech companies to argue for broader immunity – notwithstanding the intent of §230 of the Communications Decency Act, has turned the provision on its head. Rather than a shield for preventing harm, they have successfully distorted it to shield for facilitating or creating harm. Examples include near de facto near absolute immunity for claims of creating algorithms that facilitate and spread terrorism,[46] refusing to follow court orders,[47] advertising and engaging illegal firearms sales, [48] designing dating app without safety features to protect users from known dangerous conduct on its platforms including allowing other users to impersonate plaintiff and direct others to plaintiff's home for sex; [49] knowingly designing, managing, and promoting an app to be used to groom and sexually abuse minors;[50] facilitating sex trafficking,[51] creating a tool for reprogramming a computer system for cars and provided technical assistance and guidance on using the tool to defeat emission controls,[52] to name a few. One recent example is Doe v. Webgroup Czech Republic.[53] Here, the trafficked plaintiff accused defendants of knowingly receiving videos of her sexual exploitation, which were CSAM because she was a child.[54] Defendants claimed § 230 immunity for the receipt and possession of CSAM. Importantly,

---

[43] Doe v. Am. Online, 783 So. 2d 1010 (Fla. 2001).
[44] Doe v. Am. Online, 783 So. 2d 1010, 1019 (Fla. 2001)(Lewis, J., dissenting).
[45] Doe v. Am. Online, 783 So. 2d 1010, 1019 (Fla. 2001) (Lewis, J. dissenting).
[46] Force v. Facebook, 934 F.3d 53 (2d. Cir. 2019).
[47] Hassell v. Bird, 420 P.3d 776, 789 (Cal. 2018) (Yelp's refusal to comply with a court injunction is protected by Section 230).
[48] Daniel v. Armslist, LLC, 926 N.W.2d 710, 715, 726 (Wis. 2019), cert. denied. 140 S.Ct. 562 (2019) (website was immune under Section 230, despite allegations that website intentionally designed to evade federal firearm laws).
[49] Herrick v. Grindr LLC, 765 F. App'x 586 (2d Cir. 2019)
[50] Doe v. Snap, Inc. 2022 WL 2528615 (S.D. TX July 7, 2022), aff'd by 2023 WL 4174061, (5th Cir. June 26, 2023), re'h en banc den'd by 88 F.4th 1069 (5th Cir. Dec. 18, 2023).
[51] Doe v. Backpage.com, LLC, 817 F.3d 12, 16-21 (1st Cir. 2016). Plaintiffs – sex trafficking survivors who were repeatedly sold on Backpage.com, accused defendants of entering into a joint venture with sex traffickers wherein Backpage adapted posting requirements, accepted anonymous payments, advised traffickers how to avoid law enforcement, and stripped images of metadata – all to facilitate sex trafficking. Id.
[52] United States v. EZ Lynk, et.al, 2024 WL 1349224 (S.D. N.Y. March 28, 2024).
[53] No. 21-CV-02428, 2024 WL 3533426 (C.D. Cal. July 24, 2024).
[54] Id. at *6.

receipt and possession of CSAM is a federal crime, and Congress has made it also a basis for a private right of action.[55] Notwithstanding that, the district court accepted the platforms argument and found that:

> [I]nsofar as Plaintiff seeks to hold Defendants liable for "receipt" of the illicit [CSAM] videos, these claims are immune from liability under Section 230. Receipt of materials or content is, as it were, simply the first step in any publishing regime; if so, then mere receipt of illicit [CSAM] material is not sufficient to preclude immunity under Section 230.[56]

This court essentially concluded that § 230 immunizes a platform for acts that explicitly federal criminal law. Clearly, that is not the intent behind § 230's text, purpose, or history.

None of these actions remotely resemble traditional publishing duties or Good Samaritan removal of objectionable content. Yet, citing to the very early § 230 cases from the early 2000's, these courts found these platforms immune from prosecution, thereby denying victim survivors the opportunity to prove their case. One judge described courts' actions as follows:

> [F]rom the very start, courts held § 230 did much more than overrule Stratton Oakmont's publisher-liability theory. . . . Though Zeran has been criticized as inconsistent with the text, context, and purpose of § 230 . . . , the opinion was cut-and-paste copied by courts across the country in the first few years after the statute arrived.[57]

Calling the current jurisprudence a "*far cry* from what has prevailed in court" Justice Thomas lamented the "too-common practice of reading extra immunity into statutes where it does not belong… to grant sweeping protections to Internet platforms.[58] Of particular concern to Justice Thomas was the trend in courts departing from Section 230 text. "Courts have done so by awarding immunity for their own content in contrast to Section 230(c)(1) and eviscerating the narrower liability" of Section 230(c)(2)(A).[59] He has referred to platforms abuse of this provision as "[s]ocial-media platforms have increasingly used § 230 as a get-out-of-jail free card."[60] Similarly, this reality caused the Department of Justice to note that "the combination of significant technological change since 1996 and the expansive interpretation that

---

[55] 18 U.S.C. §§ 2252, 2255 (2024).

[56] WebGroup Czech Republic, 2024 WL 3533426, at *6.

[57] Anderson v. Tiktok, Inc., 116 F.4th 180, (3d Cir. 2024)(Matey J. concurring in part dissenting in part)(emphasis added).

[58] Malwarebytes, Inc. v. Enigma Software Grp. USA, LLC, 141 S. Ct. 13, 4, 7(2020) (citations omitted).

[59] Malwarebytes, Inc. v. Enigma Software Grp. USA, LLC, 141 S. Ct. 13, 7, 8, 10 (2020) (citing to Doe v. Backpage.com, LLC, 817 F.3d 12, 16-21 (1st Cir. 2016); M.A. v. Vill. Voice Media Holdings, 809 F.Supp.2d 1041, 1048 (E.D. Mo. 2011); Doe v. Bates, No. 5:05-CV-91-DF-CMC, 2006 WL 3813758, *18 (E.D. Tex., Dec. 27, 2006). Even after Justice Thomas' insights, tech has argued and some courts have agreed - refusing to look more closely at the articulated purposes of §230 of the CDA. Instead of self-correcting the widely held belief that the current breadth of the immunity exceeded the intent of Congress, courts have claimed too many companies rely on this broad interpretation and they do not want to upset this reliance. In re Facebook, 625 SW.3d 80, 91-93 (Tex. 2021); Daisuke Wakabayashi, *Legal Shield for Social Media Targeted By Lawmakers*, N. Y. TIMES (May 28, 2020), https://www.nytimes.com/2020/05/28/business/section-230-internet-speech.html. This is a stunning statement given that "the Internet industry has a financial incentive to keep Section 230 intact." Id.

[60] Doe v. Snap, Inc., 144 S. Ct. 2493, 2494 (2024) (Thomas, J., dissenting denial of certiorari) (mem.).

courts have given §230…has left online platforms immune for a wide array of illicit activity on their services."[61]

IV. The Effect of This Conscious Effort of the Tech Industry to Distort §230 of the Communications Decency Act Is Profound

The above section discussed the *result* of the §230 experiment – de facto near absolute immunity. This section discussed the *effect* of that immunity on people and on our legal systems

A. The Harm Caused to Individuals By De Facto Near Absolute Immunity Far Exceeds Congress' Worst Fears n 1996

The Senate Judiciary Committee is familiar with the statistics regarding the effect of de facto near absolute immunity and this distortion of §230 of the Communications Decency Act. Just considering CSAM, the following is indicative of the scope of the harm. Twenty-nine years after the passage of Section 230, the fears of the Senate regarding what the Intern *could* become have not only been realized, but surpassed. Focusing on CSAM alone, this illegal material is monetized and amplified by several of these platforms who do so with impunity. This evident in a review of reports to the CyberTipline. In 1998, when the CyberTipline opened it had approximately 4500 reports.[62] In 2023 the Senior Vice President for NCMEC testified before the House Oversight Committee as follows:

> In 2022, NCMEC received over 32 million reports and more than 88 million pieces of content. Last year, NCMEC received more than 36 million reports containing more than 105 million pieces of content. Since its inception over 25 years ago, the CyberTipline has received more than 186.2 million reports containing more than 530.8 million images, videos, and other content relating to child sexual exploitation. Currently, NCMEC receives on average more than 99,000 CyberTipline reports every day.[63]

In the recent years, video depictions of child sexual exploitation outpace still images of this material.[64] Their content is violent and an Interpol study found more than 60% of the images of identified children

[61] *Department of Justice's Review of Section 230 of the Communication Decency Act Of 1996* (2020), Dep't. of Just. Archives, https://www.justice.gov/archives/ag/department-justice-s-review-section-230-communications-decency-act-1996.

[62] Statement of Yiota Souras, Sr. Vice President, National Center for Missing and Exploited Children, EARN IT Act Press Conference, February 18, 2022.

[63] Testimony of John Shehan, Sr. Vice President, National Center for Missing & Exploited Children United States House Committee on Oversight and Accountability Subcommittee on Cybersecurity, Information Technology, and Government Innovation, "Addressing Real Harm Done by Deepfakes," March 12, 2024.

[64] Statement of Yiota Souras, Sr. Vice President, National Center for Missing and Exploited Children, EARN IT Act Press Conference, February 18, 2022. These trends are echoed by the Canadian Centre for Child Protection, which in 2017 averaged approximately 4000 tips per month, 98% of them being child sexual abuse imagery.); Canadian Centre for Child Protection, Survivor's Survey, Executive Summary at 1 (2017).

were prepubescent children including infants and toddlers.[65] The Department of Justice discussed the harms of being depicted in CSAM:

> When these images are placed on the Internet and disseminated online, the victimization of the children continues in perpetuity. Experts and victims agree that victims depicted in child pornography often suffer a lifetime of re-victimization by knowing the images of their sexual abuse are on the Internet forever. The children exploited in these images must live with the permanency, longevity, and circulation of such a record of their sexual victimization. This often creates lasting psychological damage to the child, including disruptions in sexual development, self-image, and developing trusting relationships with others in the future.[66]

This is echoed by survivors themselves who discuss that CSAM affects them differently than child sexual abuse, pointing to "permanence of the images and the fact that if the images are distributed, their circulation will never end."[67]

B. The Harm Caused By De Facto Near Absolute Immunity To Society and Access to Justice Is Profound

Two additional effects of de facto near absolute immunity must be noted and both relate to the courts. The first is the capacity for harm an unregulated industry possesses when those they harm do not have access to the courts. The second is the uniquely pernicious harm preclusion of discovery has for victims and society.

First, this distortion of Congressional intent with the Communications Decency Act and the undermining of Congressional action regarding trafficking, CSAM, and other forms of exploitation has shut the courthouse door to victims, states attorneys general, and others harmed. Importantly, to say that these groups are shut out of the justice system is not say they are precluded from winning at trial. They are stopped from ever being able to have their day in court because the tech industry has transformed §230 of the Communications Decency Act into a de facto near absolute immunity provision, allowing for dismissal of these causes of action at the motion to dismiss stage – prior to discovery. As Justice Thomas noted,

> Paring back the sweeping immunity, courts have read into §Section 230 would not necessarily render defendants liable for online misconduct. It simply would give plaintiffs a chance to raise their claims in the first place. Plaintiffs still must prove the merits of their cases, and some claims

---

[65] Interpol & ECPAT Int'l, **Towards a Global Indicator on Unidentified Victims in Child Sexual Exploitation Material: Summary Report** (2018)

[66] Child Pornography, **U.S. Dep't of Just.**, https://www.justice.gov/criminal-ceos/child-pornography [https://perma.cc/3M3X-BYMQ] (Aug. 11, 2023).

[67] **Captured on Film: Survivors of Child Sex Abuse Material Are Stuck in a Unique Cycle of Trauma,** Nat'l Ctr. for Missing and Exploited Child. 3 (2019).

> will undoubtedly fail. Moreover, states and the federal government are free to update their liability laws to make them more appropriate for an Internet-driven society.[68]

Part of the architecture of anti-exploitation efforts include attacking CSAM and trafficking on multiple fronts: prevention, protection, and disruption. This requires the use of criminal, civil, federal, and state tools. When companies are aware their behavior could expose them to risk of accountability, they will be deterred from illegal behavior prior to the abuse or exploitation taking place. But if, as here, they know they will never have to account for their actions, they will continue the behavior with impunity.

This is not only an injustice to individual victim survivors. Section 230 of the Communications Decency Act has been used to preclude state court prosecutions,[69] civil suits as part of statute's guaranteed private rights of action,[70] product liability civil suits,[71] and federal attempts to enforce federal regulations.[72] This is an affront to states' rights to enforce their own criminal laws, citizens' civil rights of citizens, and the right of the public to be safe from exploitative harm. Indeed, nearly all the nations attorneys' generals have come together to three times to urge Congress to amend § 230 of the Communications decency Act to allow states to enforce their criminal laws. Their recent letter noted that

> Stories of online black market opioid sales, ID theft, deep fakes, election meddling, and foreign intrusion are now ubiquitous….Current precedent interpreting the CDA, however, continues to preclude states and territories from enforcing their criminal laws against companies that, while not actually performing these unlawful activities, provide platforms that make these activities possible. Worse, the extensive safe harbor conferred to these platforms by courts promotes an online environment where these pursuits remain attractive and profitable to all involved, including the platforms that facilitate them.[73]

The second effect is what I label the **dual danger** of de facto near absolute immunity. This industry whether it be a large company or one small actor, has the capacity to cause immeasurable harm. But, notwithstanding the risk to the public welfare or individuals, it operates without any guardrails from any outside entity. In such an ecosystem, rather than being incentivized to act as a Good Samaritan, it is actually incentivized to act in a harmful manner because it has de facto near absolute immunity for its actions. Even a small company can cause tremendous damage through facilitating CSAM, human

---

[68] Malwarebytes, Inc. v. Enigma Software Grp. USA, LLC, 141 S. Ct. 13, 9-10 (2020); For a discussion of how the tech industry actively thwarted enforcement of criminal sex trafficking laws, state development of civil and criminal liability for online sex trafficking, and victim survivor civil suits, *see* Mary Graw Leary, *History Repeats Itself: The Faces Behind Sex Trafficking are More Familiar Than You Think*, 68 EMORY L. J. ONLINE 1083 (2019).
[69] *E.g.*, Dart v. Craigslist, Inc., 665 F. Supp. 2d 961, 967–68 (N.D. Ill. 2009).
[70] *E.g.*, M.A. v. Vill. Voice Media Holdings, 809 F.Supp.2d 1041, 1048 (E.D. Mo. 2011);
[71] *E.g.*, Anderson v. TikTok, 637 F.Supp 3d. 276 (2022), rev'd 116 F.4th 180, (3d Cir. 2024).
[72] *E.g.*, United States v. EZ Lynk, et.al, 2024 WL 1349224 (S.D. N.Y. March 28, 2024).
[73] https://www.naag.org/policy-letter/state-ags-support-amendment-to-communications-decency-act/

trafficking,[74] sextortion,[75] and non-consensual sexualized images.[76] With the emergence of artificial intelligence sexualized images of children and adults, the moral hazard risks are even greater.[77] Citron and Wittes convincingly note that a historical pattern exists of nascent industries beginning with no regulation but when they grow to maturity having natural guardrails in place.[78] When industries, such as transportation, utilities, and agriculture, reach a point where they can cause serious harm to large numbers of people, some form of outside oversight occurs.[79] Here with this industry, that has not occurred. Indeed, the tech industry seeks wider immunity.[80]

This is a dual danger because the risk is not only the lack of guardrails for a very powerful industry. Due to the preclusion of discovery on an industry with no oversight or guardrails, the tech industry has been able to prevent the public from learning anything about its internal workings. Undoubtedly the reason the tech industry so aggressively protects the distorted immunity is that it prevents litigants from being able to prove their cases or the public from being aware of the level of their behavior. The few occasions the public has been able to learn of partnerships between platforms and exploiters was through Congressional investigations and whistleblower. [81] This dual danger leaves the most vulnerable with no protection and no remedy for harm experienced due to the actions of an industry with de facto near absolute immunity from accountability. Furthermore, by precluding discovery it leaves those seeking to do harm anonymously and those platforms with immunity without limits to engage in behavior without limits.

---

[74] *E.g., Backpage.com's Knowing Facilitation of Online Sex Trafficking: Hearing Before the Subcomm. on Investigations*, 115th Cong. (2017); Global Report on Trafficking in Persons 2020, UNODC(referring to traffickers' use of the Internet "digital hunting fields." Katie McQue and Mei-Lin McNamara, How Facebook and Instagram Became Marketplaces for Child Sex Trafficking, The Guardian (April 27, 1993)

[75] *E.g., By The Numbers, NCMEC (noting in 2023 the CyberTipline received 186,819 reports of online enticement which includes sextortion, and increase of 323% since 2021), available at https://www.missingkids.org/theissues/sextortion#:~:text=digital%2Dediting%20tools.-,By%20the%20Numbers,enticement%20reports%20increased%20by%20323%25.*

[76] *E.g.*, Amanda Lenhard, et.al, Nonconsensual Image Sharing: One in 25 Americans Has Been A Victim of Revenge Porn, Data and Society at 5 (Dec. 13, 2016);

[77] How AI Is Being Abused to Create Child Sexual Imagery, Internet Watch Foundation (Oct. 2023), available at https://www.iwf.org.uk/about-us/why-we-exist/our-research/how-ai-is-being-abused-to-create-child-sexual-abuse-imagery/.

[78] Danielle Keats Citron & Benjamin Wittes, The Internet Will Not Break: Denying Bad Samaritans § 230 Immunity, 86 **Fordham L. Rev.** 401, 406 (2017)..

[79] Id.

[80] In 2024 tech companies continued to attempt to expand their already de facto near absolute immunity. Calise v. eta, 103 F.4th 732,742(9th Cir. 2024)("Meta invites us to reconsider the limitations we have previously recognized and encourages us to adopt a broader rule that would effectively bar 'all claims' 'stemming from their publication of information created by third parties.")

[81] *Backpage.com's Knowing Facilitation of Online Sex Trafficking: Hearing Before the Subcomm. on Investigations*, 115th Cong. (2017); Statement of Frances Haugan, U.S. Senate Commission on Commerce, Science, and Transportation, Subcommittee of Consumer Protection, Safety and Privacy Sub-Committee on Consumer Protection, Product Safety, and Data Security (Oct. 1, 2021).

V. Principles to Consider in Reform

After nearly three decades of judicial distortion of §230 of the Communications Decency Act, the results have been clear:

> The result is a § 230 that immunizes platforms from the consequences of their own conduct and permits platforms to ignore the **ordinary obligation that most businesses have** to take reasonable steps to prevent their services from causing devastating harm. But this conception of § 230 immunity departs from the best ordinary meaning of the text and ignores the context of congressional action.[82]

Therefore, Congress must act.

Such a revision should be multi-tiered to reflect this complex terrain, but not be overly unwieldy to delay enactment. Two principles the Conference Committee identified in 1996 remain relevant in today's reality: (1) companies should have protection from suit when they remove harmful content from platforms, and (2) companies should face the same liability as all other industries when they facilitate harm or create harmful products. In recent years, Congressional Committees have explored a variety of approaches. In constructing a multi-tiered revision, some promising components of reform may include, but are not limited to, aspects of the following.

First, the law should retain Good Samaritan immunity of §230(c)(2). As originally intended, an ICS should receive immunity from liability for good faith removal of material it "considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected."[83] Second, Congress should eliminate the §230(c)(1) shield while retaining Good Samaritan protection of § 230(c)(2). Any immunity beyond that for Good Samaritan removal has been distorted by tech companies and simply does not serve any of the legislation's purposes. It neither assists in limiting exploitive and indecent content, nor does it advance the development of the internet – an industry not in need of special consideration. With neither the purpose of the CDA nor Telecommunications Acts advanced, § 230(c)(1) immunity constitutes a failed experiment.

Additionally, it is important to note that this is simply a removal of immunity from suit, not a finding of liability. This simply allows those who allege a platform harmed them to have their day in court. Plaintiffs or prosecutors would still need to prove their case. But plaintiffs would be able to obtain discovery, and platforms would no longer enjoy secretive business practices they should know are

[82] Anderson v. TikTok, Inc., 116 F.4th 180, 191 (3d Cir. 2024) (Matey, J. concurring in part and dissenting in part)(emphasis added).
[83] 47 U.S.C. § 230(c)(2).

harmful and only discoverable by congressional investigations or whistleblowers. Rather, platforms will have to assess risk in business decisions similar to every other business.

The claim that this will lead to crippling litigation is unfounded. Analogously, copyright law affords such holders rights to prevent infringement online and this is carved out of §230 protections.[84] The jurisprudence in this analogous space has developed, and here companies have implemented clear notification and takedown procedures. Parties now know what a reasonable effort is to remove copyrighted material, and although § 230 does not give platforms immunity with copyrighted works, the internet still thrives. Similarly, in this area of the law affecting victims, the jurisprudence which has not been allowed to develop under a regime of de facto near absolute immunity will emerge, a reasonable duty of care will become clear, and the risks a business takes will be influenced by potential liability similar to all other industries.

Third, the internet is no longer a nascent endeavor but a massive, thriving, and self-sufficient ecosystem. As Justice Kagan raised during a recent oral argument, "every other industry has to internalize the costs of its conduct. Why is it that the tech industry gets a pass?"[85] Platforms, therefore, should be liable for facilitating, hosting, amplifying, or distributing materials that they should know are illegal or exploitive (including but perhaps not limited to CSAM, sexualized images of children, human trafficking, nonconsensual pornography, and deepfake sexualized imagery). The concept of the original § 230--that a website should not be liable as a publisher--originated because a publisher can be aware of the illegality of the content. Platforms today, unlike in 1996, collect a massive amount of data. These companies have demonstrated they are capable of leveraging vast amounts of customer data for profit and should also be required to use that data to ensure protection.[86]

Fourth, most industries are expected to exercise reasonable care in their design and function. There is no reason why this industry, which is so far reaching, should be exempt from such a requirement. By having such a standard similar to other businesses, platforms would be allowed a defense that they complied with a reasonable standard of care. This use of best practices should be a trial defense, not a source of immunity from suit. In that context, aggrieved persons would have their day in court to learn the information possessed and actions taken by the platforms who, in turn, would have an opportunity to

[84] § 230(e)(2); See, Dan Solove, Restoring the CDA Section 230 to What It Actually Says, **TeachPrivacy** (Feb. 4, 2021) (noting that while a platform is not required to remove an unconsented to nude photo, it is required to do so if the image is copyrighted).
[85] Gonzales v. Google, 598 US 617 (2023).
[86] Congress may also want to consider clarifying the mens rea of 47 U.S.C. §230(e)(5)(A) which tech has succeeded in obfuscating contrary to the intent of the amendment.

rebut the allegation by demonstrating their actions taken to prevent such harm fit within the standard of care for its particular business.

Fifth, states should be allowed to enforce their criminal laws. For several years, the National Association of Attorneys General has called upon Congress to amend § 230(e)(1) to state that "[n]othing in this section shall be construed to impair . . . any other Federal or State criminal statute."[87] The ability of states to enforce their own criminal laws against platforms who harm their citizens is essential. For example, currently, states' hands are tied when their citizens' images are distributed online by platforms in violation of state criminal laws. To preclude the ability of states to enforce criminal laws that mirror federal laws is unnecessary and harmful to victims.

Conclusion

There are many possible actions Congress can take to address online exploitation. However, the ecosystem that creates the ability to harm with such impunity stems from the distortion of §230 of the Communications Decency Act. Rather than solely draft legislation that reacts to harms occurring, the goal should be to create a safer digital space preventing such harms in the first place. This will not take place until the industry that houses the material and facilitates the harm faces accountability for their actions similar to almost every other industry.

[87] Letter from Nat'l Ass'n of Att'ys Gen. to Sen. Rockefeller, Sen. Thune, Rep. Upton, and Rep. Waxman (July 23, 2013), https://www.eff.org/files/cda-ag-letter.pdf; NAAG Supports Amendment to the Communications Decency Act, **Nat'l Ass'n of Att'ys Gen.** (May 23, 2019), https://www.naag.org/press-releases/naag-supports-amendment-to-the-communications-decency-act/ [https://perma.cc/B8HZ-S4F3] (noting support for a letter signed by forty-seven attorneys general to amend § 230 to allow the enforcement of state law).