Prepared Written Testimony

Mary Graw Leary

Professor of Law
The Catholic University of America, Columbus School of Law

Where Are We Now: Section 230 of the Communications Decency Act of 1996

House Committee on Energy and Commerce
Subcommittee on Communications and Technology

April 11, 2024

2123 Rayburn House Office Building

Introduction

Thank you for the invitation to appear before you today to discuss Section 230 of the Communications Decency Act. My name is Mary Graw Leary and I am a Professor of Law at the Catholic University of America, Columbus School of Law and currently a Visiting Professor at the University of Georgia School of Law.[1] My scholarship examines the intersection of criminal law and contemporary victimization, focusing on the exploitation of marginalized people, especially women and girls, and crime victim rights.[2] My experience includes studying these issues as an academic, but also working on issues of online exploitation with victim survivors, non-profit organizations, and other stakeholders. In this capacity I have studied the history and intent of Section 230 and several forms of exploitation including, but not limited to child sex abuse material (CSAM), human trafficking, and nonconsensual sexual material.

As we examine Section 230 nearly three decades after its passage, several realities become apparent. The original intent of Section 230 of the Communications Decency Act, while many sided, was borne out of an intent to limit the proliferation of indecent and harmful materials on the Internet. That is to say Section 230 cannot properly be understood without acknowledging the landscape of protection from indecent material and exploitation from which it emerged. This context is reflected in the text, legislative history, and contemporaneous debate.

That intent, and the Congressional intent of other legislation regarding crimes of exploitation, has been thwarted by courts erroneously reframing and de-emphasizing these purposes and, therefore, turning Section 230 on its head. The result of this judicial expansion has been a transformation from the intended limited immunity of Section 230 to a *de facto* near absolute immunity far beyond what Congress envisioned.[3] The consequences of this have been devastating for victims of exploitation and the public. The effects have been felt both in the courtrooms across the country where victim survivors and prosecutors are denied access to justice and outside these courtrooms where platforms continue to amplify and monetize exploitation in many forms. After years of inaction, the time has come for Congress to hear

[1] The views expressed are my own and not those of either The Catholic University of America or The University of Georgia.
[2] *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).
[3] See e.g., Section 230 — Nurturing Innovation or Fostering Unaccountability?, U.S. Dep't of Just. ("[C]ourts have interpreted the scope of Section 230 immunity very broadly, diverging from its original purpose.").

the growing chorus of judges and stakeholders dismayed by the state of jurisprudence and return Section 230 to its original purpose and address today's Internet and the harms Section 230 has caused.

I. A Brief History of Section 230

Some of the difficulty in discussing "Section 230" is in just that very description: "Section 230." Technology companies and their surrogates often ignore the statute's clear context and instead describe it as a stand-alone piece of legislation designed to protect the Internet, rather than an intentional component of the Communications Decency Act. However, properly understood, it must be read in its full context both textually and historically. Textually, it was passed within the Obscenity and Violence Title (Title V) of the Telecommunications Act of 1996.[4] It specifically addresses the obligation of interactive computer services (ICS) to block and screen offensive material as is demonstrated by its title, "Protection for Private Blocking and Screening of Offensive Material."[5] This textual orientation quite intentional and the legislative history demonstrates that Section 230 is only properly understood as one that emerges from a landscape of protection from explicit material.[6]

A. Legislative History

In 1996 Congress set out to update the outdated 62-year-old Communications Act of 1934. At that time Congress sought to adjust its regulatory framework to the "new" issues such as cable television, digital communication, and a nascent dial up World Wide Web. The Internet of today was unimaginable in 1996 when only 20% of users went online every day, the average American spent less than 30 minutes a month exploring the Internet, dial up was the main form of connection, and less than 45 million people worldwide used it.[7] Social media was not yet the norm with Facebook, Twitter, Snap, or TikTok not emerging until 2004 and later. The Supreme Court characterized sexually explicit material as available but "seldom encountered accidentally."[8]

Even at that time, however, many members of Congress were aware of the risks of platforms expanding explicit and harmful material, cyberstalking, and adult sexual offenders gaining unprecedented access to children.[9] A revised Communications Decency Act emerged from the Senate in 1996 as part of

[4] Telecommunications Act of 1996, Pub. L. No. 104, 110 Stat. 56 (1996).
[5] 47. U.S.C. § 230.
[6] As will be discussed infra, that is not to say that protection is the only purpose of Section 230, but that it emerges from this landscape of protection.
[7] Reno v. A.C.L.U, 521 U.S. 844, 850 (1997); Farhad Manjoo, *Jurassic Web*, Slate (Feb. 24, 2009.
[8] Reno v. A.C.L.U, 521 U.S. 844, 854 (1997).
[9] *E.g.*, 141 CONG. REC. S1954 (daily ed. June 9, 1995).

the Telecommunication Act, and it was designed to address these concerns.[10] This effort to limit the spread of explicit material was shared by many as the bill passed the Senate 81-18. Even those who opposed the bill primarily did so regarding a separate section unrelated to Section 230 and later found unconstitutional. Notwithstanding that, even these opponents recognized the CDA was designed from a protective framework and shared the goal to "protect children from obscene and indecent material."[11]

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 case, *Stratton Oakmont v. Prodigy Services Co*.[12] Prodigy operated a financial services bulletin board where people could post information about the financial sector and it attempted to monitor the board for inappropriate content. Stratton Oakmont sued for defamation regarding an anonymous post on this board accusing it of fraudulent practices. In contrast to precedent and reality,[13] this state court agreed with Stratton Oakmont and found Prodigy responsible for that third party content in part because of Prodigy's active screening out any material it found inappropriate.[14] The court labeled 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."[15] Counterintuitively, Prodigy was held responsible because it attempted to monitor its board while in previous cases similarly situated platforms were not considered publishers of such third party content.[16] Concerned with a system that would punish a company for monitoring its platform, two members of the House proposed the Internet Freedom and *Family Empowerment Act* of 1995 (IFFE)(emphasis added). As the name suggests, this sought to address *Stratton Oakmont* which penalized a platform for actually monitoring *content* while at the same time trying to respond to the CDA approach to indecent material.

---

[10] 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.").

[11] *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," and penalize child pornographers, but also have a functioning Internet.).

[12] 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.)

[13] 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).

[14] 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.)

[15] 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)).

[16] 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, Damnum Absque Injuria, Zeran v. AOL and Cyberspace Defamation Law, 9 FORDHAM INTELL. PROP., MEDIA AND ENT. L.J. 775 (1999)

The IFFE, therefore, reflected a concern that courts could hold platforms responsible for content they did not create and disincentivize them from monitoring their platforms.[17] However, limiting the available of indecent material remained a backdrop of the discussion with this bill not just for liability at the point of distribution.

Consequently, two different versions of the Telecommunications Act emerged from each chamber of Congress. The CDA, while recognizing the value of the Internet,[18] sought to protect children and families from explicit content and to be an obstacle to child abuse and exploitation. The IFFE, while acknowledging the concerns of the CDA, wanted to encourage platforms to monitor their sites and provide families with protection. It is essential then to understand the text of Section 230 as emerging from this landscape of protection. When the Conference Committee, after months of negotiation, introduced the Telecommunications Act of 1996 in February it embraced both approaches to protecting children by including the text of the IFFE within the CDA under Section 230. This compromise legislation placing the IFFE *into* the CDA in Section 230 must be read in this context as being anchored in shielding the Internet from indecent materials.[19]

While technology companies, their surrogates, and even authors of the IFFE at times try to divorce Section 230 from these roots, that is exactly how it was situated within the law as it emerged from Conference. Contemporary Congressional debate around the legislation reflects that Title V- which housed these IFFE concepts as a component of the CDA – reflects this child protection landscape.[20] To be sure, the Telecommunication Act of 1996 has many goals within its 107 pages.[21] But much of the debate around Title V makes clear that proponents and opponents alike understood it to possess elements

---

[17]"[T]he statute's fundamental principle is that content creators should be liable for any illegal content they create." 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).

[18]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.").

[19] 141 CONG. REC. S2011, ¶ 11. The Committee Report listed as a resolved issue "cyberporn: requires operators of computer networks to screen out indecent material for children; carriers of indecent material will not be liable for the content of information generated by others…"

[20] 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).

[21]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."); The bill was described as "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.

of exploitation protection.[22] One Senator noted that "the Conference Report contains strong protections for America's children."[23] Opponents perhaps did not like some aspects of the bill, but clearly discussed Section within the context of child protection and limiting a proliferation of explicit material on the new Internet.[24] One judge described this history of Section 230 by noting that "[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."[25] Therefore, consistent with the legislative history of Title V, Congress passed Section 230 as part of the CDA, and part of a larger discussion regarding the pathways to prevent distribution of sexually explicit material and exploitation.

B. The Text of Section 230 Reflects This Legislative History

As mentioned, Congress's placement of the Communications *Decency* Act within the *Obscenity and Violence* title and the *Obscene, Harassing,* and *Wrongful Utilization of Telecommunications* Subtitle all reflect this history and intent.[26] Similarly, the renaming of this provision to *Protection for Private Blocking and Screening of Offensive Material* further demonstrates this legislation was not a stand alone bill designed for broad immunity.[27] Of the five statements discussing the policy of the United States two of them speak of promoting a vibrant Internet with limited government regulation.[28] However, the remaining three reflect this landscape of limiting access to objectionable material, encouraging user control, incentivizing blocking and filtering technologies, and vigorous enforcement of federal criminal

[22] *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.").
[23] *E.g.*, 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.").
[24] *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 is already subject to criminal penalties – obscenity, child pornography, and child exploitation via computer networks are already criminal acts.")
[25] 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.
[26] Telecommunications Act of 1996, Pub. L. No. 104, 110 Stat. 56 (1996)
[27] 47 U.S.C. 230. The statute also contains findings about the promise of the Internet and personal control over information. 47 U.S.C. § 230(a).
[28] 47 U.S.C. § 230(b)(3),(4),(5).

laws regarding obscenity, stalking, and harassment.[29] This concern about exploitive harm is essential to understanding what kind of immunity Section 230 of the CDA sought to provide. That is unquestionably limited immunity. If there were any debate, Section 230(e) explicitly mentions that these provisions should have no effect on, *inter alia*, the enforcement of federal laws regarding obscenity, sexual exploitation of children, or "any other Federal criminal statute."[30]

It is within this context of protective measures and encouraging companies to engage in conduct like Prodigy and try to block and filter inappropriate material that the two relevant sections of Section 230 rest. Under the provision labeled Protection for *good Samaritan Blocking and Screening of Offensive Material* Congress included limited immunity for such actions. First, in Section 230(c)(1) it states that providers or users of interactive computer services shall not be treated as the publisher or speaker of any information provided by a third party. Justice Thomas, in a dissent from a denial of certiorari discussed this language as intentional, noting that publishers in the common law are subjected to strict liability because they have an opportunity to edit and control the information they publish. Distributors, on the other hand, "were thus liable only when they knew (or constructively knew) that content was illegal."[31] The idea that this provision provides some sort of broad immunity is belied by the text and the goals of the legislation. Furthermore, Section 230(c)(2) provides immunity for any action "voluntarily taken in good faith to restrict access to or availability of material that the provider or user concerns to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected."[32] Consequently, the legislative history and the text demonstrate that Section 230 of the Communications Decency Act sought limited immunity for good Samaritans for monitoring their platforms.

C. Contemporary Promises By the Technology Industry

The idea that such a provision intended broad immunity is also belied by contemporary news coverage of the debate and lobbying efforts at the time which demonstrates the promises technology companies and their surrogates made in order to obtain this limited immunity. The discussion was not *whether* to protect the public from exploitive and explicit material but *how* to do so. The Wall Street Journal described IFFE as providing a system free of government regulation only "if they [ICS's] take

[29] 47 U.S.C. § 230(b)(3),(4),(5).
[30] 47 U.S.C. § 230(e). In 2018 Congress amended this section to also include that Section 230 was intended to have no effect on sex trafficking law including federal civil claims and state criminal laws when the violation would also be violations of federal sex trafficking laws. 47 U.S.C. § 230(e)(5).
[31] Malwarebytes, Inc. v. Enigma Software Grp. USA, LLC, 141 S. Ct. 13, 14, 208 L. Ed. 2d 197 (2020) (Thomas, J).
[32] The statute also provides immunity for actions to make available the technical means to restrict such access. 47 U.S.C. 230(c)(2)(B).

steps to control smut."[33] The New York Times agreed the IFFE and CDA were proposals from different perspectives, but both "intended to shield children from pornography in words and pictures as well as from other material deemed objectionable that is distributed over the Internet."[34] The technology industry's preference that, if protection had to be considered, it occur at point of receipt not distribution hinged upon the promise that technology companies would produce workable tools to filter out such material.[35]

Therefore, the media coverage reflects that Congress considered two different approaches to the problem of explicit content within the emerging medium and Congress ultimately combined them to utilize both federal law and business incentives to most effectively shield this content and prevent exploitation.

II. The History of Courts Turning This Congressional Intent on Its Head

A. Early Caselaw

Notwithstanding this clear intent for a limited immunity for good Samaritans, the judiciary through some early rulings has interpreted these provisions - with the vast assistance of technology industry and its surrogates - to offer a very broad immunity.[36] This was in part due to an unbalanced and, therefore, inaccurate focus on the non-child protective purposes of Section 230 in the very first case to be litigated. In *Zeran v. America Online*,[37] the Fourth Circuit addressed the defamation liability for the internet service provider, America Online (AOL). In so doing, the court focused on the policies of §230 relating to freedom from regulation and tort liability, but failed to discuss the other policies.[38] It's characterization of the immunity as "broad" has taken

---

[33]Daniel Pearl, *House Leaders Seek Other Ways To Fight Smut on Internet*, WALL ST. J., June 21, 1995, at B2; see also Kara Swisher and Elizabeth Corcoran, *Gingrich Condemns On-Line Decency Act,* Wash.Post, June22, 1995, at D8.

[34]Steve Lohr, *Conservatives Split On How To Regulate The Internet*, N. Y. TIMES, Dec. 4, 1995.

[35]Kara Swisher and Elizabeth Corcoran, *Gingrich Condemns On-Line Decency Act*, WASH. POST, June 22, 1995, at D8; Steve Lohr, *Conservatives Split On How To Regulate The Internet*, N. Y. TIMES, Dec. 4, 1995 ("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."); Robert Corn-Revere, *New Age Comstockery,* 4 COMM. L. CONSPECTUS 173, 174 (1996).

[36] For a comprehensive discussion of this jurisprudence as it relates to sex trafficking *see* Mary Graw Leary, *The Indecency of the Communication Decency Act*, 41 Harv. J. L. Pub. Pol'y 553, 574-581 (2018).

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

[38] 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. (emphasis added) However, it never explained the other purposes of §230 which demonstrate the very limited immunity and that qualifier has largely been ignored.

on a life of its own and has led to an assertion that any allegation that involves a third party implicates immunity under Section 230. Not until recently have judges began calling for a return to the text and for Congress acknowledged the error of this path and correct it.[39]

With technology companies and their surrogates throughout the country seizing on this language in its litigation, 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 not only defamation cases, but cases finding immunity for the allegation that AOL knowingly distributed and allowed advertisements for CSAM and a failed to respond to notification that its services were being utilized to distribute obscene material. [40] The concerns of the dissent in that case forewarned this would create "carte blanche immunity for wrongful conduct plainly not intended by Congress."[41] His concerns were well placed.

This concept of *de facto* near absolute immunity for their conduct has led to platforms being considered immune for their conduct has led to immunity from more and more claims having little or nothing to do with publishing. These cases include giving platforms de facto near absolute immunity for claims of creating algorithms that facilitate and spread terrorism,[42] refusing to follow court orders,[43] advertising and engaging illegal firearms sales, [44] 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; [45] knowingly designing, managing, and promoting an app to be used to groom and

[39] *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).
[40] Doe v. Am. Online, 783 So. 2d 1010 (Fla. 2001).
[41] Doe v. Am. Online, 783 So. 2d 1010, 1019 (Fla. 2001) (Lewis, J. in dissent).
[42] Force v. Facebook, 934 F.3d 53 (2d. Cir. 2019).
[43] Hassell v. Bird, 420 P.3d 776, 789 (Cal. 2018) (Yelp's refusal to comply with a court injunction is protected by Section 230).
[44] 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).
[45] Herrick v. Grindr LLC, 765 F. App'x 586 (2d Cir. 2019).

sexually abuse minors;[46] and facilitating sex trafficking[47] to name a few. None of these actions remotely resembled traditional publishing duties or the kind of good Samaritan immunity Congress envisioned. 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 and their government the opportunity to prove their case.[48] This reality caused the Department of Justice to note that "the combination of significant technological change since 1996 and the expansive interpretation that courts have given §230…has left online platforms immune for a wide array of illicit activity on their services."[49]

B. The Growing Chorus of Judges Questioning This Approach

As mentioned, in an early CSAM case, Judge Lewis, writing in dissent, forewarned of the error in over reliance on *Zeran*.

> 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….[50]

He found the majority's blind following of Zeran "frustrate[d] the core concepts explicitly furthered by the Act and contravene[d] its express purpose . . . . [T]he so-called Decency Act has, contrary to well established legal principles been transformed from an appropriate shield

[46] 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).

[47] 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. 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).

[48] United States v. EZ Lynk SEZC, et.al, 2024 WL 1349224 (S.D. N.Y. March 28, 2024). Just last week a federal district court precluded in part under Section 230 of the Communications Decency Act the United States government from enforcing Section 203 of the Clean Air Act against defendants who allegedly created a tool for reprogramming a computer system for cars and provided technical assistance and guidance on using the tool to defeat emission controls. Id. In so doing the court noted, "It is not the role of this Court to rewrite a statute, and refuse to apply precedent, to avoid an outcome that Congress might not have foreseen in 1996 and the executive dislikes today." Id. at *1.

[49] *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.

[50] Doe v. Am. Online, 783 So. 2d 1010, 1019 (Fla. 2001) (Lewis, J. in dissent).

into a sword of harm."[51] For many years many courts have accepted the litigation position of the platforms and few courts questioned this claim of broad immunity. However, there is a growing chorus of judges calling on courts to revisit Section 230 and restore it to its original intent and for Congress to update it reflect the modern day Internet.

Some cases have accepted this assertion of broad immunity, but denied immunity due to certain platform's conduct.[52] The Washington State Supreme Court was the first court that allowed a sex trafficking case proceed past the motion to dismiss stage on state law grounds, but as important was its concurring opinion.[53] Justice Wiggins, wrote separately to clarify that plaintiffs' claims did not treat Backpage as a publisher or speaker and to vehemently reject Backpage and the dissent's view that Section 230 provides immunity to such actions by a platform.[54]

Similarly, Chief Justice Katzmann, writing in the dissent in *Force v. Facebook*, also challenged the majority opinion's granting of immunity in an anti-terrorism civil suit.[55] He noted the absurdity that Section 230 "was designed to encourage computer service providers to shield minors from obscene material so that it now immunizes those same providers for allegedly connecting terrorists to one another."[56] This dissent has been adopted by a growing number of judges calling for a reexamination of this incorrect interpretation of Section 230 in light of the actual text of the provision.[57]

---

[51] Doe v. Am. Online, 783 So. 2d 1010, 1019 (Fla. 2001) (Lewis, J. in dissent).

[52] J.S. v. Vill. Voice Media Holdings, 359 P.3d 714 (Wash. 2015) (en banc); Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157, 1163 (9th Cir. 2008).

[53] J.S. v. Vill. Voice Media Holdings, 359 P.3d 714 (Wash. 2015) (en banc).

[54] J.S. v. Vill. Voice Media Holdings, 359 P.3d 714, 718 (Wash. 2015)(Wiggins, J., concurring)

[55] Force v. Facebook, 934 F.3d 53, 77 (Katzmann, C.J., dissenting).

[56] Even its sponsor stated that "it is firmly established in the caselaw that §230 cannot act as a shield when encouraging a website to be in any way complicit in the creation or development of illegal content." Christopher Cox, *The Origins and Original Intent of Section 230 of the Communications Decency Act*, U. OF RICHMOND J. L. AND TECH. (Aug. 27, 2020), https://jolt.richmond.edu/2020/08/27/the-origins-and-original-intent-of-section-230-of-the-communications-decency-act/.

[57] E.g., Gonzalez v. Google LLC, 2 F.4th 871, 913 - 918 (9th Cir. 2021), vacated and remanded, 598 U.S. 617, 143 S. Ct. 1191, 215 L. Ed. 2d 555 (2023), and rev'd sub nom. Twitter, Inc. v. Taamneh, 598 U.S. 471, 143 S. Ct. 1206, 215 L. Ed. 2d 444 (2023)(Berzon, J., concurring); Id. at 920 (Gould, J. concurring in part, dissenting in part). These voices calling for a course correction in the judiciary at times take the form of a dissent but at other times note their hands are tied due to this precedent.[57] Gonzalez v. Google LLC, 2 F.4th 871, 913 (9th Cir. 2021), vacated and remanded, 598 U.S. 617, 143 S. Ct. 1191, 215 L. Ed. 2d 555 (2023), and rev'd sub nom. Twitter, Inc. v. Taamneh, 598 U.S. 471, 143 S. Ct. 1206, 215 L. Ed. 2d 444 (2023)(Berzon, J. concurring)("Although we are bound by Ninth

Recently 7 of 15 judges from the Fifth Circuit Court of Appeals dissented from a denial of rehearing *en banc* asking their colleagues to revisit its "sweeping immunity for social media companies that the text cannot possibly bear."[58] In so doing they noted that "[i]t strains credulity to imagine that Congress would simultaneously impose distributor liability on platforms in one context, and in the same statute immunize them from that very liability."[59]

Most notably Justice Thomas lamented the current state of jurisprudence regarding Section 230 in a statement accompanying a denial of a petition for writ of certiorari.[60] In *Malwarebytes, Inc. v. Enigma Software Group USA, LLC*, Justice Thomas agreed with the denial of certiorari, but wrote separately to invite reconsideration of whether the actual text of Section 230 "aligns with the current state of immunity enjoyed by Internet platforms."[61] Returning to the actual intent and text of Congress in 1996, he described the immunity as a "*limited* protection [that] enables companies to create community guidelines and remove harmful content without worrying about legal reprisal."[62] Referencing the law's response to *Stratton Oakmont*, he noted that Section 230(c)(1) does not make an ISP a publisher by simply hosting third party content and Section 230(c)(2)(A) provides immunity when companies take good faith steps to decrease access to objectionable material.[63] Calling the current jurisprudence a "*far cry* from what has prevailed in court" he lamented the "too-common practice of reading extra immunity into statutes where it does not belong… to grant sweeping protections to Internet platforms."[64]

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

Circuit precedent compelling the outcome in this case, I join the growing chorus of voices calling for a more limited reading of the scope of section 230 immunity.").

[58] Doe through Roe v. Snap, Inc, 88 F.4th 1069, 1070 (5th Cir. 2023) (Elrod, J. dissenting from denial of rehearing en banc).

[59] Doe through Roe v. Snap, Inc., 88 F.4th 1069, 1070 (5th Cir. 2023) (Elrod, J. dissenting from denial of rehearing en banc).

[60] Malwarebytes, Inc. v. Enigma Software Grp. USA, LLC, 141 S. Ct. 13 (2020).

[61] Malwarebytes, Inc. v. Enigma Software Grp. USA, LLC, 141 S. Ct. 13, 14 (2020).

[62] Malwarebytes, Inc. v. Enigma Software Grp. USA, LLC, 141 S. Ct. 13, 14 (2020) (emphasis added).

[63] Malwarebytes, Inc. v. Enigma Software Grp. USA, LLC, 141 S. Ct. 13, 14 (2020).

[64] Malwarebytes, Inc. v. Enigma Software Grp. USA, LLC, 141 S. Ct. 13, 15 (2020) (citations omitted) (emphasis added).

Section 230(c)(1) and eviscerating the narrower liability" of Section 230(c)(2)(A).[65] The effect of these actions is widespread.

IV. The Effects of Expanding Limited Immunity to De Facto Near Absolute Immunity Are Profound Both Within Society and Within Courthouses

A. Effects Outside the Courtroom

The experiment these courts have advanced of de facto near absolute immunity has failed. Twenty-eight years after the passage of Section 230, the fears of the Senate have not only been realized, but surpassed. Nowhere is this more apparent than with regard to CSAM. This illegal material is not only available but monetized and amplified by several of these platforms who do so with impunity.[66] This is evident in a review of reports to the CyberTipline. In 1998, when the CyberTipline opened it had approximately 4500 reports.[67] Just two weeks ago, the Senior Vice President for NCMEC testified before the House Oversight Committee as follows:

> In 2022, NCMEC received over 32 million reports [to the CyberTipline] 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.

---

[65] Malwarebytes, Inc. v. Enigma Software Grp. USA, LLC, 141 S. Ct. 13, 17 (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 courts have refused to look more closely at the articulated purposes of Section 230. Instead of self-correcting the widely viewed belief 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.").

[66] At a January Senate Judiciary Hearing, one senator noted that while Meta sometimes sends a warning to a user that the content they are about to view is possibly CSAM but then allows the user to continue to view CSAM. Big Tech and the Ongoing Child Sexual Abuse Crisis: Hearing Before the Committee on the Judiciary (January 31, 2024(Comments of Senator Cruz), available at https://www.judiciary.senate.gov/committee-activity/hearings/big-tech-and-the-online-child-sexual-exploitation-crisis; Nicholas Kristof, *The Children of Pornhub*, New York Times (Dec. 4, 2020), available at https://www.nytimes.com/2020/12/04/opinion/sunday/pornhub-rape-trafficking.html?smid=tw-share.

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

> Currently, NCMEC receives on average more than 99,000 CyberTipline reports every day.[68]

In the recent years, video depictions of child sexual exploitation outpace still images of this material.[69]

Other forms of exploitation are thriving on the Internet and include human trafficking,[70] sextortion,[71] non-consensual pornography,[72] and of most recent discussion generative artificial intelligence sexualized images of children and adults.[73]

It is not only the quantity of material that has proven the harm of *de facto* near absolute immunity, it is also the quality of harm. The suffering experienced by victim survivors of these exploitive crimes suffering is lifelong and can include trauma, depression, difficulty in romantic/sexual relationships, difficulty in friendship, physical suffering including injury and somatic effects feelings of psychological distress, and (emotional isolation, anxiety, and fear) and permanent revictimization.[74] Most recently the alarm has been sounded regarding generative AI CSAM and sexualized imagery.[75] The problem is so severe that the F.B.I. issued a

---

[68] 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.

[69] 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).

[70] *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 as "digital hunting fields"); Katie McQue and Mei-Lin McNamara, How Facebook and Instagram Became Marketplaces for Child Sex Trafficking, The Guardian (April 27, 2023).

[71] *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.

[72] *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).

[73] 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/.

[74] *E.g.*, Canadian Centre for Child Protection, Survivor's Survey, Executive Summary at 9,28, 29 (2017); Captured on Film, SURVIVORS OF CHILD SEX ABUSE MATERIAL ARE STUCK IN A UNIQUE CYCLE OF TRAUMA, National Center for Missing and Exploited Children (2019), available at https://www.missingkids.org/content/dam/missingkids/pdfs/Captured%20on%20Film.pdf; *Child Pornography*, U.S. Dept. of Just., https://www.justice.gov/criminal-ceos/child-pornography (last visited Apr. 4, 2022).

[75] For a more thorough discussion of the quantity and harms experienced by survivors of this exploitation see Testimony of John Shehan, Sr. Vice President, National Center for Missing & Exploited Children United States

public warning about the practice of criminals maliciously creating photographs to target individuals.[76]

B. Effects Within Courthouses

Not only are the effects of *de facto* near absolute immunity felt throughout society often by the most vulnerable. But they are felt in courthouses around the nation. It is critical to understand the effect of immunity. In the hundreds of cases platforms assert immunity, they do so at the motion to dismiss stage. What that means is they are able to have the cases dismissed prior to having to exchanging any discovery material. Immunity, as opposed to a trial defense means that the case is dismissed without the victim survivors ever having the ability prove their case in court. In a cruel twist, victim survivors are initially harmed when platforms amplify or monetize their victimization. Then, when they seek to hold said platforms accountable, the platform is able to dismiss the claim precluding it from every having to disclose information in discovery which could further prove the victim survivor's claim. Victim survivors are denied the most basic opportunity to prove their cases through obtaining internal documents from the only people who have those documents: the platforms. Justice Thomas recognized this reality noting that, "[p]aring 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 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."[77]

Indeed, one of the few occasions the public has been able to learn of partnerships between platforms and exploiters was after a two-year Congressional investigation into Backpage.com.[78] Similarly, Congress and the public have only learned of the scope of internal

House Committee on Oversight and Accountability Subcommittee on Cybersecurity, Information Technology, and Government Innovation, "Addressing Real Harm Done by Deepfakes," March 12, 2024.

[76] Malicious Actors Manipulating Photos and Videos to Create Explicit Content and Sextortion Schemes, F.B.I. (June 5, 2023), https://www.ic3.gov/Media/Y2023/PSA230605 (last visited April 7, 2024).

[77] Malwarebytes, Inc. v. Enigma Software Grp. USA, LLC, 141 S. Ct. 13, 18 (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).

[78] *Backpage.com's Knowing Facilitation of Online Sex Trafficking: Hearing Before the Subcomm. on Investigations*, 115th Cong. (2017).

awareness by platforms of the known danger to children and design defects of their products from whistleblowers from within some of these companies.[79]

This is not only an injustice to individual victim survivors. Section 230 has been used to preclude state investigations,[80] civil suits as part of statute's guaranteed private rights of action,[81] product liability civil suits,[82] and federal attempts to enforce federal regulations.[83] This raises important questions of the civil rights of citizens, the state right to enforce its own criminal laws, and the right of the public to be safe from exploitative harm. Indeed, nearly all the nations attorneys' general have come together three times to urge Congress to amend Section 230 to allow states to enforces their criminal laws. Their most recent letter noted that

> [s]tories 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.[84]

An addition effect has been highlighted by Professor Danielle Citron who has noted that the immunity regime has prevented the development of caselaw responsive to deliberate profiteering from wrongdoing which would which will provide guidance to businesses on what liability is reasonable.[85] This additional negative effect of an underdeveloped caselaw has served neither potential victim survivors or businesses seeking to establish acceptable business practices.

Therefore, the chorus of voices calling for a return of Section 230 to its original intent crosses many sectors to include victim survivors of various harms caused directly from platforms' actions, federal and state officials who find themselves powerless to exercise their

---

[79] Statement of Frances Haugen, U.S. Senate Committee on Commerce, Science, and Transportation, Subcommittee on Consumer Protection, Product Safety, and Data Security (Oct. 1, 2021); Statement of Arturo Bejar, U.S. Senate Committee on the Judiciary, Subcommittee on Privacy, Technology and the Law (Nov. 7, 2023).
[80] *E.g.*, Dart v. Craigslist, Inc., 665 F. Supp. 2d 961, 967–68 (N.D. Ill. 2009).
[81] *E.g.*, M.A. v. Vill. Voice Media Holdings, 809 F.Supp.2d 1041, 1048 (E.D. Mo. 2011);
[82] *E.g.*, Anderson v. TikTok, 637 F.Supp 3d. 276 (2022).
[83] *E.g.*, United States v. EZ Lynk, et.al, 2024 WL 1349224 (S.D. N.Y. March 28, 2024).
[84] https://www.naag.org/policy-letter/state-ags-support-amendment-to-communications-decency-act/
[85] Danielle Keats Citron, How to Fix Section 230, 103 Boston U. L.Rev 713, 719 (2023).

rights or enforce their own laws, and members of the public confronted with the reality of today's Internet both directly creating harm through its model of profit based on extreme content.

V. Potential Features of Reform

The time is uniquely compelling to return Section 230 to its original purpose. Society faces unprecedented 21st Century problems that cannot be adequately addressed with a 20th Century tool. This is particularly true when that tool has been transformed from its original protective purpose to a sword that not only fails to protect but exacerbates some of the very harms sought to be avoided. The time is also now because of the growing chorus of judges, victim survivors, and stakeholders asking Congress to assist in correcting the misdirected jurisprudence which has advanced an immunity for conduct unimagined in 1996.

While this Committee has many options, I suggest the Committee consider exploring the following features of reform. Such a revision should be multi-tiered to reflect the complexity of the landscape, but not overly bureaucratic to delay enactment. First, the law should retain the good Samaritan immunity of Section 230(c)(2). As originally intended, an ICS should receive immunity from liability for good faith restriction or 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."[86] Second, any further statutory immunity should be eliminated for both civil suits by victim survivors or enforcement of state laws (for acts also illegal under federal law) and such businesses face the same accountability measures as other entities. *De facto* near absolute immunity simply does not serve any of the purposes of Section 230. The Internet is no longer a nascent endeavor in need of assistance to thrive but a massive ecosystem capable of inflicting serious harm.[87] Platforms, therefore, should be responsible for their conduct of facilitating criminal or exploitive material by hosting, amplifying, or distributing materials that they know or should know are illegal or exploitive (including but perhaps not limited to CSAM, sexualized images of children, human trafficking, non-consensual pornography, and "deepfake" imagery).[88] They should be incentivized to

[86] 47 U.S.C. § 230(c)(2).
[87] *See*, Danielle Keats Citron and Benjamin Wittes, The Internet Will Not Break: Denying Bad Samaritans §230 Immunity, 86 Fordham L. Rev. 401 (2017).
[88] As Justice Thomas notes, a possible background concept of Section 230 was the distinction between a publisher and a distributor and the reality that a publisher is in the position to know content is illegal and, therefore, held to a higher standard. Malwarebytes, Inc. v. Enigma Software Grp. USA, LLC, 141 S. Ct. 13, 14 (2020). Given the

marshal their business of collecting, sorting, and selling data not only for profit, but for protective purposes as well, including engaging in safety by design principles during development and deployment of products.[89] Third, to address some of the concerns of ICS's they, like other businesses, should be allowed a trial defense that they complied with a reasonable standard of care.[90] This should be a trial defense, not a source of immunity from civil suit or liability for criminal violations of state law which mirror federal offenses. Therefore, those harmed are not denied an opportunity to hold a platform accountable for harmful business practices often causing significant lifelong damage due to failures of design, facilitation of crime, or partnership with bad actors. However, ICS's are not strictly liable for such harms but have a viable defense by establishing that their practices complied with the relevant standard of care. While perhaps outside the scope of Section 230, this standard of care could be developed by a regulatory framework governed by an existing federal agency.[91] Such a standard could create regulatory standards for safety by design, public safety, transparency, reporting requirements, and removal. This system would replace the current ecosystem of *de facto* near absolute immunity which encourages profit seeking actions with impunity.

Conclusion

The Committee should be commended for examining the goals of Section 230 of the Communications Decency Act and Section 230's ability to realize those goals in the modern world. It is clear that Section 230, while addressing many aspects of the then nascent Internet, emerged from a landscape of protection from explicit content and exploitation. After nearly three decades of evidence of courts perverting this statute from an intended limited immunity to a system of *de facto* near absolute immunity and the effects of such a regime have been dramatic.

---

ability of these platforms to marshal a significant amount of data on their users and use that information for profit, there certainly may be occasions when they know or should know of the content and should be incentivized to act as though they risk liability for inaction.

[89] Many scholars and organizations have recognized that a system of self-regulation has failed. *See e.g*., OSCE, Policy Responses to Technology Facilitated Trafficking in Human Beings, 28-29 (2022).

[90] See Letter to Congressman Frank Pallone from Alliance to Counter Crime Online (Sept. 8, 2021); Neil Fried, et.al, *Section 230 Reform Naysayers Ignore Clear Problems Online-and the Clear Solutions*, Tech Policy Press (October 13, 2021), available at https://www.techpolicy.press/section-230-reform-naysayers-ignore-clear-problems-online-and-the-clear-solutions/; Danielle Keats Citron, How to Fix Section 230, 103 Boston U. L.Rev 713, 753 (2023).

[91] The OSCE issued a comprehensive analysis of technology facilitated human trafficking and concluded that self-regulation has not been successful and state led regulatory frameworks are "desperately needed." OSCE, Policy Responses to Technology-Facilitated Trafficking in Human Being, 54 (2022).

The result has been not only the thwarting of Congressional goals, but facilitating a level of exploitation surpassing even Congress' greatest fears. Section 230 should be returned to its original purpose to address this reality.