Catholic University Law Review

Volume 68
Issue 3 *Summer 2019*

Article 11

2019

From Innovation to Abuse: Does the Internet Still Need Section 230 Immunity?

Benjamin Volpe

From Innovation to Abuse: Does the Internet Still Need Section 230 Immunity?

Cover Page Footnote
J.D., The Catholic University of America, Columbus School of Law, 2019; M.P.S., The George Washington University, College of Professional Studies, 2009; B.A., Cedarville University, 2007. I would like to thank Professor Chris Savage for his expert guidance and feedback during the process of writing this Comment.

FROM INNOVATION TO ABUSE: DOES THE INTERNET STILL NEED SECTION 230 IMMUNITY?

Benjamin Volpe[+]

> "The [i]nternet is the first thing that humanity has built that humanity doesn't understand, the largest experiment in anarchy that we have ever had."
>
> – Eric E. Schmidt, Board of Directors, Alphabet Inc.[1]

I. INTRODUCTION

In American jurisprudence, online entities such as websites and social media platforms have broad immunity to turn a blind eye to illegal, harmful, and tortious activity that occurs via their online services, at the expense of the unwary consumer.[2] When a 13-year-old girl meets a sexual predator online, leading to a sexual assault, the website that facilitated interactions leading to the assault enjoys immunity from tort liability.[3] Twitter is immune from liability for allowing terrorist groups to use its platform to spread extremist propaganda, raise funds, attract recruits, and ultimately carry out attacks.[4] And notoriously, multiple children have been trafficked in the sex trade through the use of online classified websites, but after finding their freedom, were unable to hold the

---

[+] J.D., The Catholic University of America, Columbus School of Law, 2019; M.P.S., The George Washington University, College of Professional Studies, 2009; B.A., Cedarville University, 2007. I would like to thank Professor Chris Savage for his expert guidance and feedback during the process of writing this Comment.

1. Graham Singer, *In Hindsight...Infamous Tech Industry Predictions and Quotations*, TECHSPOT (Nov. 16, 2017), https://www.techspot.com/article/754-tech-predictions-and-quotes/ (quoting Eric E. Schmidt, ex-Google CEO, Alphabet Board of Directors).

2. *See* Michael L. Rustad & Thomas H. Koenig, *Rebooting Cybertort Law*, 80 WASH. L. REV. 335, 370 (2005). "Websites can facilitate defamation, pornography, and wholesale invasions of privacy without the risk of tort liability." *Id.* at 373.

3. In *Doe v. Myspace*, the child's parent sued Myspace, an internet social networking website, for negligence and strict product liability after the child's assault, asserting that Myspace should have had safety measures in place to protect children against predators. *See* Doe v. Myspace, 629 F. Supp. 2d 663 (E.D. Tex. 2009). Myspace prevailed on a motion to dismiss after the court found it was not an information content provider—thus immune under § 230 of the Communications Decency Act. *See id.* at 664. *But see* Doe v. Internet Brands, Inc., 824 F.3d 846 (9th Cir. 2016) (holding the Communications Decency Act did not immunize a modeling website from tort liability when rapists utilized the website to lure girls into fake modeling auditions where they were drugged, raped, and filmed because the website was not treated as a publisher of content in the failure to warn claim).

4. Fields v. Twitter, Inc., 217 F. Supp. 3d 1116, 1120 (N.D. Cal. 2016).

website operators liable for the role they played as facilitators and co-profiteers in the venture.[5]

There are many other stories like these, where predators, bullies, fraudsters, and criminals have harmed innocent people because of a lack of reasonable safeguards on the internet. Victims are unable to obtain justice due to the challenging reality of locating anonymous defendants and overcoming the high wall of § 230 immunity for internet intermediaries.[6] Moreover, the proliferation of fake news and foreign countries waging silent wars through disinformation campaigns online raises the question—are we doing enough to protect ourselves online?[7]

After the Industrial Revolution, tort law developed into a means to enforce protections for consumers of mass produced food and automobiles as well as railroad and factory workers.[8] In this new "negligence era," tort law responded to death and disaster on a massive scale "as turnpikes and burgeoning industry were vastly accelerating the pulse of activity and confronting society with an

5. This is the story of Doe v. Backpage.com, LLC, 817 F.3d 12 (1st Cir. 2016). In that case, three minors who survived nearly 1000 sexual assaults at the behest of sex traffickers sued Backpage.com, an online classifieds website, for violations of the federal Trafficking Victims Protection Reauthorization Act of 2008 and its state equivalent as well as the state unfair and deceptive business practices law, among other claims. *Id.* Backed by amici curiae filings from several state officials and human rights groups, the plaintiffs lost because of § 230 immunity, even with evidence that Backpage.com tailored its website to make sex trafficking easier, profited from sponsoring the sex trafficking ads, and charging a posting fee for them. *See* Doe v. Backpage.com, LLC, 817 F.3d 12, 17, 29 (1st Cir. 2016). This was one of the online sex trafficking lawsuits that made headlines, spurring Congress to act by closing the loophole of § 230 immunity for online sex trafficking facilitators in 2018. *See* Pub. L. No. 115-164, 132 Stat. 1253–56, Apr 11, 2018.

6. For a discussion of cases applying § 230 immunity, see Rustad & Koenig, *supra* note 2, at 372 n.169–176. *See*, *e.g.*, Doe v. GTE Corp., 347 F.3d 655 (7th Cir. 2003) (applying § 230 immunity to defendant web host that allegedly hosted a voyeur website that posted nude videos of the plaintiffs); Ramey v. Darkside Prods., No. 02-730, 2004 U.S. Dist. LEXIS 10107 (D.D.C. May 17, 2004) (applying § 230 immunity to defendant adult services advertising website that allegedly posted intimate photos of plaintiff without her permission); Ben Ezra, Weinstein, & Co. v. America Online, Inc., 206 F.3d 980, 983 (10th Cir. 2000) (applying § 230 immunity to defendant internet service provider for providing internet access to a third party who posted defamatory information about plaintiff); Doe v. Am. Online, Inc., 783 So. 2d 1010, 1011 (Fla. 2001) (applying § 230 immunity to defendant internet service provider after suit by mother of 11-year-old boy who was lured into sexual conduct, photographed, and videotaped by online predator).

7. *See generally* Jennifer Williams-Alvarez, *Facebook, Twitter, Google Counsel Testimony: Russian Influence Broader Than Initially Thought*, THE RECORDER (Nov. 1, 2017, 2:55 AM), https://www.law.com/corpcounsel/sites/corpcounsel/2017/10/31/facebook-twitter-google-counsel-testimony-russian-influence-broader-than-initially-thought/; Jennifer Williams-Alvarez, *Google GC Kent Walker Joins Tech Counsel for Day 2 of Congressional Grilling*, THE RECORDER (Nov. 2, 2017, 2:55 AM), https://www.law.com/therecorder/sites/corpcounsel/2017/11/01/google-gc-kent-walker-joins-tech-counsel-for-day-two-of-congressional-grilling/.

8. *See* Rustad & Koenig, *supra* note 2, at 363-64; *see also* W. PAGE KEETON ET AL., PROSSER AND KEETON ON THE LAW OF TORTS § 81, at 580-83 (5th ed. 1984); Irwin A. Horowitz, Norbert L. Kerr & Keith E. Niedermeier, *Jury Nullification: Legal and Psychological Perspectives*, 66 BROOKLYN L. REV. 1207, 1218 (2001).

accident problem of hitherto unprecedented dimensions."[9] Thus, if the "[i]nternet Revolution is the new Industrial Revolution,"[10] then certain types of consumer harm unique to the internet context are sure to follow, requiring tort law to hold actors liable for negligently omitting reasonable safety precautions.[11]

In 1996, Congress passed the Communications Decency Act (CDA)[12] in part to allow the internet to flourish "with a minimum of government regulation[,]"[13] "to preserve the vibrant and competitive free market that presently exists for the [i]nternet and other interactive computer services,"[14] and "to ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of a computer."[15] Section 230 of the Communications Act (part of the CDA) provides what the common law majority in the United States considers to be immunity when three elements are met: "[1] the defendant [is] a provider or user of an 'interactive computer service'; [2] the asserted claims . . . treat the defendant as a publisher or speaker of information; and [3] the information [is] provided by another 'information content provider.'"[16]

---

9. Rustad & Koenig, *supra* note 2, at 364 n.112; *see also* Danielle Keats Citron & Benjamin Wittes, *The Internet Will Not Break: Denying Bad Samaritans Section 230 Immunity*, 86 FORDHAM L. REV. 401, 422 (2017) ("The nature of the litigation protection that is essential in the early life of an industry is very different from the proper protection given to a mature one. Many people forget now that the automobile industry had nearly total product-liability protection in tort for deaths and injuries in car crashes through the 1960s—even when they resulted from known defects that manufacturers declined to fix. As the industry matured, the liability protection weakened, and cars became 'dramatically safer.'").

10. Micha Kaufman, *The Internet Revolution is the New Industrial Revolution*, FORBES (Oct. 5, 2012, 3:42 PM), https://www.forbes.com/sites/michakaufman/2012/10/05/the-internet-revolution-is-the-new-industrial-revolution/#705ca54547d5.

11. For a discussion comparing the development and maturation of industrial tort law (such as the automobile industry) with internet law, *see* Citron & Wittes, *supra* note 8, at 420–23. Citron & Wittes argue that the current internet liability regime under § 230 "lacks any kind of sensible allocation of risk[,]" removing incentives for online providers and websites to engage in any reasonable standard of care required by other industries. *Id.*

12. Pub. L. No. 104-104, 110 Stat. 133-39, §§ 502–09, Feb. 8, 1996. The relevant parts discussed in this Comment are § 502 (amending 47 U.S.C. § 223 (1994)) and § 509 (codified at 47 U.S.C. § 230 (2012)).

13. 47 U.S.C. § 230(a)(4) (2012).

14. *Id.* § 230(b)(2). The CDA defines an interactive computer service as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the [i]nternet and such systems operated or services offered by libraries or educational institutions." *Id.* § 230(f)(2).

15. *Id.* § 230(b)(5).

16. Schneider v. Amazon.com, Inc., 31 P.3d 37, 39 (Wash. Ct. App. 2001). *See also* 47 U.S.C. § 230 (2012) ("Protection for 'Good Samaritan' blocking and screening of offensive material. (1) Treatment of publisher or speaker. No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider. (2) Civil liability. No provider or user of an interactive computer service shall be held liable on account of—(A) any action voluntarily taken in good faith to restrict

Although much of the CDA was struck down as unconstitutional on First Amendment grounds,[17] § 230 of the Act remains as a declaration of Congress's 1996 policy choice to make the internet free and unregulated.[18] Unsurprisingly, not everybody is comfortable with a policy choice that effectuates broad immunity to internet service providers, website operators, and website hosts. For example, some state governments have resorted to guerilla tactics to regulate internet companies by using a practice known as "jawboning."[19] Furthermore, with cases capturing national headlines, such as the Backpage.com line of cases,[20] Congress has recently initiated a fresh look at § 230 immunity. In 2018, Congress passed the Allow States and Victims to Fight Online Sex Trafficking Act of 2017, which clarifies that § 230 "was never intended to provide legal protection to websites that unlawfully promote and facilitate prostitution and websites that facilitate traffickers in advertising the sale of unlawful sex acts with sex trafficking victims."[21]

However well-intentioned the CDA is and however successful it has been at promoting the free market on the internet, the dangers of a wholly-unregulated, free-range internet in the interconnected modern world are growing too great to ignore.[22] Leaving internet self-regulation to the discretion of companies

---

access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or (B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1)."). An "information content provider" is defined as "any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the [i]nternet or any other interactive computer service." *Id.*

17. *See* Reno v. A.C.L.U., 521 U.S. 844, 864 (1997); *see also infra* Section I.B.

18. *See infra* text accompanying note 41.

19. *See* Derek E. Bambauer, *Against Jawboning*, 100 MINN. L. REV. 51, 57–58 (2015). "Jawboning" is "a specific type of informal pressure by a government actor on a private entity: one that operates at the limit of, or outside, that actor's authority." A good example of jawboning is when state governments sent demand letters to Backpage.com, threatening litigation if they did not comply with what amounted to informal regulation of their adult services ads, forcing Backpage.com to choose whether to comply with the unlawful demands (pre-empted by § 230) or incur the costs of litigation. *Id.* at 67–69.

20. *See*, *e.g.*, Florida Abolitionist v. Backpage.com LLC, No. 6:17-cv-00218, 2017 U.S. Dist. LEXIS 75744 (M.D. Fla. May 18, 2017); Complaint, Sojourner Center v. Backpage.com LLC, Docket No. 2:17-cv-00399 (D. Ariz. Feb. 7, 2017), ECF No. 1; Doe v. Backpage.com, LLC, 817 F.3d 12 (1st Cir. 2016); J.S. v. Vill. Voice Media Holdings, LLC, 359 P.3d 714 (Wash. 2015); Backpage.com, LLC v. Cooper, 939 F. Supp. 2d 805 (M.D. Tenn. 2013).

21. Pub. L. No. 115-164, 132 Stat. 1253, § 2, Apr. 11, 2018.

22. *See generally, e.g.*, Barnes v. Yahoo!, Inc. 570 F.3d 1096 (2009) (illustrating the problem of revenge porn); David S. Levine, *Confidentiality Creep and Opportunistic Privacy*, 20 TUL. J. TECH. & INTELL. PROP. 11 (2017) (discussing Russian exploitation of Facebook advertising to influence U.S. election); *Sen. Klobuchar Issues Statement on Russian Bought Political Google Ads,* TARGETED NEWS SERVICE, (LEXIS) (Oct. 9, 2017, 3:53 AM) (discussing Russian exploitation of Google ads to spread disinformation); *Texas: First Circuit Affirms Dismissal of Lawsuit Against Backpage.com, Confirms Broad Scope of Section 230 Immunity*, U.S. OFFICIAL NEWS (LEXIS), (Mar. 21, 2016) (discussing Backpage.com classifieds used for sex trafficking of minors); *Young*

accountable to stockholders and profits presents a dangerous conflict with the legitimate interests of consumers. Unfortunately, due to the majority approach in American courts—a broad immunity interpretation of § 230 immunity—many victims of internet-related crimes and abuse have been left without meaningful recourse in tort law.[23]

This Comment will examine cyber tort law and discuss the history and purpose of the CDA. In doing so, this Comment provides legislative background along with an accounting of the common law history of the CDA, specifically related to § 230 immunity of internet service providers and online intermediaries (interactive computer services).[24] Three main approaches to the interpretation of internet liability vis-à-vis § 230 have emerged: companies are bound by strict liability (pre-1996 approach in the U.S.), companies have blanket immunity (majority approach), and companies have conditional immunity (Seventh and Ninth Circuit approaches).[25]

This Comment will analyze each of these approaches and recommend a solution that more carefully balances the interests of large internet-based companies with consumer protection. Congress should re-evaluate the language and stated intent of § 230, making new findings in light of the modern, technologically-interconnected world. Moreover, this Comment argues that the 2018 amendment to § 230 did not go far enough. Congress should make more comprehensive policy statements in § 230 regarding consumer safety online and intermediary liability, and should amend § 230 to implement a notice-takedown procedure similar to the European model and that of the Digital Millennium Copyright Act (DMCA), thereby establishing a new standard of care to hold internet companies accountable to.

Victims of Cyberbullying Twice as Likely to Attempt Suicide and Self-Harm, Study Finds, MEDICAL XPRESS (LEXIS), (Aug. 16, 2017, 12:51 PM) (discussing cyberbullying on social media and related suicides); *More Than a Quarter of UK Women Experiencing Online Abuse and Harassment Receive Threats of Physical or Sexual Assault New Research*, FOREIGN AFFAIRS (LEXIS), (Nov. 21, 2017) (discussing the prevalence of online harassment, abuse, and threats).

23. *See* Citron & Wittes, *supra* note 8, at 413 (discussing how the broad immunity given to online service providers removes any duty of care to the consumer, "giv[ing] online platforms a free pass to ignore illegal activities, to deliberately repost illegal material, and to solicit unlawful activities while ensuring that abusers cannot be identified[,]" often immunizing providers from activities that extend beyond internet speech).

24. For the purposes of this Comment, the CDA's term "interactive computer service," defined *supra* note 13, will be used interchangeably with terms such as "online intermediaries," defined *infra* note 53. It appears this is what courts have done, although arguments might be made that different standards of liability should be applied to an internet service provider, for example, versus a small website operator. *See* Rustad & Koenig, *supra* note 2, at 371 ("Courts have extended the meaning of 'interactive computer services,' haphazardly lumping together web hosts, websites, search engines, and content creators into this amorphous category.").

25. *See infra* Section II.D for an analysis of a general fourth approach to interactive computer service liability—the negligence or notice-based standard (European model and Digital Millennium Copyright Act approach). Although these liability regimes fall outside the purview of § 230, they are analyzed in this Comment for their comparative value.

II. THE PROGRESSION AND MODERNIZATION OF INTERNET LIABILITY POLICY

Congress passed the Telecommunications Act of 1996[26] "[t]o promote competition and reduce regulation in order to secure lower prices and higher quality services for American telecommunications consumers and encourage the rapid deployment of new telecommunications technologies."[27] Title 5 of that Act, entitled the Communications Decency Act of 1996,[28] amended § 223 of the Communications Act of 1934[29] by setting criminal penalties for transmitting or displaying obscene materials to minors via the use of an interactive computer service[30] and offering immunity to those who solely provide network access or connection (not including those who create "the content of the communication").[31] Furthermore, the Act provided a good faith defense for anyone who implemented "good faith, reasonable, effective, and appropriate actions" to "restrict or prevent access by minors" to obscene materials on the internet.[32]

A. Legislative Underpinnings of the Communications Decency Act

The CDA was introduced by Senator Exon, who had no experience with the internet,[33] to shield minors from indecency—especially pornography—on the internet.[34] The CDA was codified under Title 47, "Telegraphs, Telephones, and

---

26. The Telecommunications Act of 1996 made several amendments to the Communications Act of 1934.

27. Pub. L. No. 104-104, 110 Stat. 56, Feb. 8, 1996. The legislative history further reveals that in passing § 230, Congress wanted "to overrule *Stratton-Oakmont v. Prodigy* and any other similar decisions which have treated such providers and users as publishers or speakers of content that is not their own because they have restricted access to objectionable material." H.R. REP. NO. 104-458, at 194 (1996) (Conf. Rep.). Congress believed decisions such as Stratton Oakmont, Inc. v. Prodigy Servs. Co., No. 31063/94, 1995 N.Y. Misc. LEXIS 229 (May 24, 1995) discussed *infra*, disempowered parents from "determin[ing] the content of communications their children receive through interactive computer services." *Id.* Interestingly, however, the Conference agreement specifically states that § 230 immunity does not "apply to so-called 'cancelbotting,' in which recipients of a message respond by deleting the message from the computer systems of others without the consent of the originator or without having the right to do so." *Id.*

28. § 501, 110 Stat. at 133.

29. *See* 47 U.S.C. § 223 (1994).

30. § 502, 110 Stat. at 133.

31. *Id.*

32. *Id.*

33. Robert Cannon, *The Legislative History of Senator Exon's Communications Decency Act: Regulating Barbarians on the Information Superhighway*, 49 FED. COMM. L.J. 51, 53, 72 (1996).

34. 142 CONG. REC. S714, S718 (daily ed. Feb. 1. 1996) (statement of Sen. Exon) ("[I introduced the CDA] to protect children from indecent, pornographic communications on the [i]nternet and other computer services and to protect all Americans from computer obscenity and electronic stalking. With the passage of this bill, the Congress will help make the Information Superhighway safer for kids and families to travel. The current lawlessness on the [i]nternet has opened a virtual Triple-X (XXX)-rated bookstore in the bedrooms of every child with a computer. This law alone will not clean up the [i]nternet. Parental supervision, industry co-operation along

Radiotelegraphs," § 223, "Obscene or harassing phone calls in the District of Columbia or in interstate or foreign communications."[35]

The CDA was enacted with multiple safe harbor provisions under § 223 to dampen the blow of its radical approach against obscenity on the internet.[36] Congress intended that internet service providers should be immune from suit as long as their function was to provide online access, not to create content.[37] Senator Exon explained:

> The legislation generally does not hold liable any entity that acts like a common carrier without knowledge of messages it transmits or hold liable an entity which provides access to another system over which the access provider has no ownership of content . . . Congress does not hold the mailman liable for the mail that he[] delivers.[38]

Thus, it seems clear that the CDA's safe harbor provisions, created in the incipiency of the boom of personal internet use, were originally thought to safeguard and responsibly facilitate a new market for internet service providers by protecting them from vicarious liability.[39]

Before the enactment of § 223, however, two additional pieces of legislation were introduced to complement § 223. First, the Family Empowerment Amendment, which gave "Good Samaritan" protection to providers or users of interactive computer services that block or screen "offensive material" on the internet,[40] was introduced in response to Senator Exon's § 223 as a way to ensure protection against government regulation.[41] Later codified under § 230, the

---

with strict law enforcement, need to work together to make this exciting new technology the family friendly resource that it should be.").

35. 47 U.S.C. § 223 (2000); *see also* Cannon, *supra* note 33, at 72–73 (musing how a senator with no internet experience can draft a bill regulating it); *see also infra* Section III.A.

36. Matthew Schruers, Note, *The History and Economics of ISP Liability for Third Party Content*, 88 VA. L. REV. 205, 213–14 (2002); *see also* Cannon, *supra* note 33, at 59–60 (discussing Congress adding defenses to the original version of § 223 amidst strong pressure from the "interactive computer service industry").

37. 142 CONG. REC. H1158 (daily ed. Feb. 1, 1996) (statement of Rep. Hyde).

38. 142 CONG. REC. S714 (daily ed. Feb. 1. 1996) (statement of Sen. Exon).

39. H.R. REP. NO. 104-458, at 190 (1996) (Conf. Rep.).

40. Pub. L. No. 104-104, 110 Stat. 137-38, § 509, Feb. 8, 1996.

41. Cannon, *supra* note 33, 67–68. The stated policy goals of the Family Empowerment Act, later codified under 47 U.S.C. § 230(b) are 5-fold:

> (1) to promote the continued development of the [i]nternet . . .
>
> (2) to preserve the vibrant and competitive free market that presently exists for the [i]nternet and other interactive computer services, unfettered by . . . regulation . . .
>
> (3) to encourage the development of technologies which maximize user control . . .
>
> (4) to remove disincentives for the development and utilization of blocking and filtering technologies . . .
>
> (5) to ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer.

Family Empowerment Act did little more than overrule the 1995 *Stratton Oakmont, Inc. v. Prodigy Servs. Co.* decision that held an internet service provider liable for defamatory comments posted by a third party on a website.[42] As such, the Family Empowerment Act became known as the "bill without a verb."[43] It was criticized for not actually forbidding government regulation of the internet;[44] but merely allowing congressmen to shallowly "declare their allegiance to the First Amendment and cyberspace without actually committing themselves to legislation of significance."[45]

Second, Congressman Bliley quietly introduced another amendment to the House version of the Telecommunications Act on the day of the vote.[46] This amendment, known as the "Manager's Amendment," altered the telecommunications bill "to appease the interests of big business" by extending CDA protections to interactive computer services under § 230.[47]

The Commerce Department, Federal Communications Commission, and Justice Department uniformly opposed the CDA. The Justice Department voiced concerns that the CDA would make it difficult to prosecute obscenity on the internet.[48]

B. Interpretations of the Communications Decency Act and Internet Tort Liability

Roughly a year after the enactment of the CDA, the Supreme Court, in *Reno v. A.C.L.U.*, struck down Senator Exon's § 223 on First Amendment grounds, holding that it was an impermissibly vague, over-inclusive, overly-broad, content-based regulation on speech, likely to "interfere with the free exchange of ideas."[49] In *Reno*, the Court opined that because "the [i]nternet is not as 'invasive' as radio or television [is in a person's home]," it has not been subject to the same level of government regulation.[50] Concurring in part and dissenting

---

§ 509, 110 Stat. at 138.

42. *See* Cannon, *supra* note 33, at 68; *see also* discussion *infra* Part II. As codified under 47 U.S.C. § 230, the Family Empowerment Act clarified that interactive computer service providers "shall not be treated as the publisher[s] or speaker[s] of any information provided by another information content provider." Pub. L. No. 104-104, 110 Stat. 138, § 509, Feb. 8, 1996;

43. Cannon, *supra* note 33, at 69.

44. *Id.* at 68.

45. *Id.* at 69.

46. *Id.*

47. *Id.*; *see* § 509, 110 Stat. at 133–34; 141 CONG. REC. H8452, H8456 (daily ed. Aug. 4, 1995) (statement of Rep. Bryant) (lamenting that the last minute introduction of the Manager's Amendment, drafted in private by corporate interests, without the public's input, is "an embarrassment to the House"). Section 230 provides protection from civil liability to "Good Samaritan" interactive computer service providers or users who essentially filter, *inter alia*, obscene or harassing materials from the internet. § 509, 110 Stat. at 134.

48. Cannon, *supra* note 33, at 69–70.

49. Reno v. A.C.L.U., 521 U.S. 844, 864, 868, 874, 879, 885 (1997).

50. *Id.* at 868–69.

in part, Justice O'Connor explained that, in her view, the CDA is "little more than an attempt by Congress to create 'adult zones' on the [i]nternet[,]" which, although not necessarily unconstitutional, are unconstitutional as set out in the CDA.[51]

Thus, although § 230 originally came paired with § 223 (to appease § 223's opposition), as a result of *Reno*, it now survives alone as the sole remnant of the CDA, along with its Good Samaritan immunity provision.[52] Since *Reno*, courts have wrestled with interpreting § 230's Good Samaritan provision in internet contexts stretching far beyond § 223's contemplation of pornography, indecency, and obscenity. Three main approaches have emerged over the past 20+ years regarding tort liability for interactive computer services and internet intermediaries.[53]

First, prior to the enactment of § 230, courts in the United States held interactive computer services to a strict liability standard. Second, § 230 expressly countermanded the strict liability approach, replacing it with liability protections for interactive computer services—later interpreted by many courts as a broad immunity for those service providers. Third, some courts more recently have interpreted § 230 as providing immunity to interactive computer services, on the condition they have not participated in the production or development of the alleged harmful content.

1. Pre-CDA: Strict Liability for Online Content Publishers

Prior to the passage of the CDA in 1996, government officials considered "imposing strict liability on ISPs [internet service providers] as a means for

---

51. *Id.* at 886 (O'Connor, J., concurring in part and dissenting in part). Justice O'Connor elaborates:

> Our cases make clear that a 'zoning' law is valid only if adults are still able to obtain the regulated speech. If they cannot, the law does more than simply keep children away from speech they have no right to obtain—it interferes with the rights of adults to obtain constitutionally protected speech and effectively 'reduces the adult population . . . to reading only what is fit for children.

Id. at 888.

52. Schruers, *supra* note 36, at 213–14.

53. Internet intermediaries are:

> private entities that host or index online content. . . . [i]nternet intermediaries wield considerable control over what we see and hear today, akin to that of influential cable television and talk radio shows. Examples include search engines like Google, Microsoft, and Yahoo!; browsers like Mozilla; social network sites like Facebook . . . ; micro-blogging services like Twitter; video-sharing sites like YouTube; and newsgathering services like Digg.

Danielle Keats Citron & Helen Norton, *Intermediaries and Hate Speech: Fostering Digital Citizenship for Our Information Age*, 91 B.U.L. REV. 1435, 1438–39 (2011); *see also* Zeran v. Am. Online, Inc., 129 F.3d 327, 330–31 (4th Cir. 1997) ("Congress made a policy choice . . . not to deter harmful online speech through the separate route of imposing tort liability on companies that serve as intermediaries for other parties' potentially injurious messages.").

controlling some of the [i]nternet's dangers."[54] Soon, courts in the United States held interactive computer services on the internet to a strict liability[55] publisher standard for torts such as defamation.[56]

In *Cubby v. Compuserve*, Cubby, a database operator running a journalism forum sued Compuserve, a competing database operator, alleging that the journalism forum run by Compuserve published several defamatory statements regarding Cubby's service.[57] The district court granted the defendant's motion for summary judgment because it acted as an unwitting distributor of information (not a publisher), much like a bookseller, and had no reason to know of the presence of the defamatory statements.[58] Recognizing strict liability for publishers of information online, the *Cubby* court thus announced that "the appropriate standard of liability . . . is whether [the defendant] knew or had reason to know" of the harmful content.[59]

In *Stratton Oakmont*, a New York trial court tackled the question of to whom liability attaches for defamatory messages posted by a third party on an online message board.[60] In this case, Prodigy Services, an early internet service provider, moderated and operated an online message board about financial products.[61] When an unidentified third party posted defamatory comments on the message board, the defamed parties sued Prodigy Services.[62] In defense, Prodigy Services argued that it was merely a distributor (similar to a bookstore or library) of the online content, not a publisher (similar to a newspaper); and thus, it could incur no liability for content posted on its message board.[63]

However, because Prodigy advertised itself to the public as screening the content posted on its websites for "family friendly" qualities, by way of moderators and filtering software, the court found Prodigy to have exercised

---

54. Ronald J. Mann & Seth R. Belzley, *The Promise of Internet Intermediary Liability*, 47 WM. & MARY L. REV. 239, 247 (2005).

55. Strict liability is defined as:

> liability in tort imposed on an actor (including a commercial enterprise) for the harms the actor causes, whether or not the actor is negligent. "Enterprise liability" is synonymous with strict liability, except that the former phrase connotes a broader commitment to holding commercial enterprises strictly liable for the harm they cause—some would say "characteristically cause"—as a matter of first principle.

James A. Henderson, Jr., *Why Negligence Dominates Tort*, 50 UCLA L. REV. 377, 380 (2002).

56. Schruers, *supra* note 36, at 232. "Strict liability is the equivalent of publisher liability, since publisher liability holds publishers strictly liable for the content of their publications, regardless of their knowledge." *Id.*

57. Cubby, Inc. v. Compuserve, Inc., 776 F. Supp. 135, 138 (S.D.N.Y. 1991).

58. *Id.*

59. *Id.* at 139–41.

60. Stratton Oakmont v. Prodigy Servs. Co., No. 31063/94, 1995 N.Y. Misc. LEXIS 229 (N.Y. Sup. Ct. May 24, 1995).

61. *Id.* at *1–3.

62. *Id.*

63. *Id.* at *6–7.

editorial control over the content, similar to a newspaper publisher.[64] Alluding to the difference between active online providers versus passive online providers, the court stated: "[Prodigy's] conscious choice, to gain the benefits of editorial control, has opened it up to a greater liability than . . . other computer networks that make no such choice."[65] In its finding, the court recognized "the issues addressed herein may ultimately be preempted by federal law if the Communications Decency Act . . . , several versions of which are pending in Congress, is enacted."[66]

Distinguished in later cases, and effectively overruled by § 230 of the CDA,[67] *Stratton Oakmont* became known for its application of a strict liability publisher standard to an internet service provider.[68] In *Zeran v. America Online, Inc*, 129 F.3d 327 (4th Cir. 1997), the Fourth Circuit opined that strict liability for interactive computer services creates a disincentive for such companies to self-regulate, because it would impose publisher liability upon any service provider that attempts to regulate offensive material on their services—exactly the type of positive citizenship Congress sought to promote by passing § 230 of the CDA.[69] Because of § 230's Good Samaritan provision and the *Zeran* holding, strict liability became an obsolete approach to cyber tort liability.

2. Post-CDA: Broad Immunity for Interactive Computer Services

Another view, most widely seen in post-1996 case law, is that the CDA gives broad immunity[70] to any interactive computer service that is not the information content provider[71] (publisher or speaker) of alleged tortious content. Contrary to the strict liability regime of *Stratton Oakmont*, courts taking this approach give broad immunity to interactive computer services, even if they edit or alter content provided by third parties.[72]

---

64. *Id.* at *6–13.

65. *Id.* at *13.

66. *Id.* at *14.

67. H.R. REP. NO. 104-458, at 194 (1996) (Conf. Rep.) ("One of the specific purposes of this section is to overrule *Stratton Oakmont v. Prodigy* and any other similar decisions which have treated such providers and users as publishers or speakers of content that is not their own because they have restricted access to objectionable material. The conferees believe that such decisions create serious obstacles to the important federal policy of empowering parents to determine the content of communications their children receive through interactive computer services.").

68. *See* Zeran v. Am. Online, Inc., 129 F.3d 327, 331 (4th Cir. 1997).

69. *Id.*

70. Rustad & Koenig, *supra* note 2, at 377; *see also*, Backpage.com, LLC v. Cooper, 939 F. Supp. 2d 805, 822 (M.D. Tenn. 2013) ("[c]ourts across the country have repeatedly held that the CDA's grant of immunity should be construed broadly.") (citation omitted).

71. *See supra* note 15.

72. Adeline A. Allen, *Uber and the Communications Decency Act: Why the Ride-Hailing App Would Not Fare Well Under § 230*, 18 N.C. J. L. & TECH. 290, 309 (2017) (citing Batzel v. Smith, 333 F.3d 1018, 1031 (9th Cir. 2003)); Ben Ezra, Weinstein, & Co. v. Am. Online, Inc., 206 F.3d 980, 986 (10th Cir. 2000); Barrett v. Fonorow, 799 N.E.2d 916, 926–27 (Ill. App. Ct. 2003); and Donato v. Moldow, 865 A.2d 711, 726 (N.J. Super. Ct. App. Div. 2004)).

In *Zeran*, the Fourth Circuit considered whether an interactive computer service should face liability for failing to remove defamatory material posted online using its service, when the defamed party provided notice to the interactive computer service of the defamatory material.[73] Here, the Fourth Circuit found that § 230 gives an interactive computer service broad immunity.[74] According to the court, broad immunity is preferable to notice-based liability, for example, because notice-based liability "reinforces service providers' incentives to restrict speech and abstain from self-regulation[,]" contrary to the purposes of § 230.[75] Instead, § 230 should "encourage computer service providers to self-regulate the dissemination of offensive material over their services."[76] Moreover, tort liability imposed on interactive computer services "would have an obvious chilling effect" on internet speech.[77]

Recognizing further that organizations under a notice liability regime would have to make immediate editorial decisions every time notice is given regarding a potentially defamatory statement, the *Zeran* court opined that such a regime would give rise to "an impossible burden in the [i]nternet context."[78] Moreover, a policy of notice-based liability could give third parties "a no-cost means to create the basis for future lawsuits" by simply giving notice to internet companies each time something on the internet displeases them, with full knowledge the company faces an impossible burden in addressing the multitudinous other similar complaints.[79]

In 2014, a Texas appellate court had occasion to apply *Zeran's* broad immunity doctrine. In *GoDaddy.com, LLC v. Hollie Toups*, plaintiffs sued GoDaddy.com, an internet domain registrar and web hosting company, for hosting websites that feature sexually explicit photographs of plaintiffs, without

73. *Zeran*, 129 F.3d at 327.

74. *Id.* at 330. ("By its plain language, § 230 creates a federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service.").

75. *Id.* at 333.

76. *Id.* at 331. The court also recognized that "[Section] 230 forbids the imposition of publisher liability on a service provider for the exercise of its editorial and self-regulatory functions"—yet another departure from the publisher strict liability era of *Stratton Oakmont*. *Id.* Even more, the court recognized that § 230 also protects distributors, not just publishers. *Id.* at 332. Once the potential plaintiff provides notice of the presence of defamatory material to the interactive computer service, the computer service transforms from the role of distributor to publisher, because it must now make editorial decisions—"whether to publish, edit, or withdraw the posting"—explicitly bringing it within the protection of § 230. *Id.* at 332.

77. *Id.* at 331.

78. *Id.* at 333. Ostensibly, the court's analysis here depends on the idea that millions of internet users publishing such a vast amount of content on the internet would create an editorial burden that internet providers simply cannot reasonably bear. *See* Reno v. A.C.L.U., 521 U.S. 844, 850 (1997).

79. *Zeran*, 129 F.3d at 333.

their consent.[80] Conceding that GoDaddy.com did not create the offending images, the plaintiffs nevertheless sued for negligence, *inter alia*, on a theory that GoDaddy.com was aware of the content, failed to remove it, and profited from it.[81] Plaintiffs also alleged that GoDaddy.com hosted these websites with full knowledge the websites were engaged in illegal activities, such as the publication of child pornography.[82] The court found that because Congress did not make an exception to § 230 immunity for tort claims brought under criminal statutes, such claims are barred.[83]

In similar fashion, many courts over the past few years have applied the words of § 230 very literally, often dismissing lawsuits at the outset whenever an interactive computer service has been sued for a cause of action in tort.[84]

3. Chipping Away at Broad Immunity: Conditional Immunity for Interactive Computer Services

The third general approach courts have taken in interpreting § 230 immunity is "conditional immunity."[85] This approach gives interactive computer services broad immunity for torts related to third party content, but conditions that immunity on "minimal responsibilities implicit in Section 230."[86] In 2008, two

80. GoDaddy.com, LLC v. Hollie Toups, 429 S.W.3d 752, 753 (Tex. App. 2014). This is a case of revenge porn. Revenge porn is defined as: "sexually explicit images of a person posted online without that person's consent especially as a form of revenge or harassment." *Revenge Porn*, MERRIAM-WEBSTER DICTIONARY, https://www.merriam-webster.com/dictionary/revenge%20porn (last visited Nov. 4, 2017).

81. *GoDaddy.com*, 429 S.W.3d at 753.

82. *Id.*

83. *Id.* at 760; *see also*, Doe v. Myspace, Inc. 474 F. Supp. 2d 843 (W.D. Tex. 2007) *aff'd*, 528 F.3d 413 (5th Cir. 2008) (finding § 230 immunity is not limited to defamation lawsuits, but also applies to negligence, negligence per se, intentional infliction of emotional distress, invasion of privacy, civil conspiracy, and distribution of child pornography suits); Doe v. Mark Bates, No. 5:05-CV-91, 2006 U.S. Dist. LEXIS 93348, at *12 (E.D. Tex. Dec. 27, 2006) ("Congress decided not to allow private litigants to bring civil claims based on their own beliefs that a service provider's actions violated the criminal laws.").

84. *See*, *e.g.*, Fields v. Twitter, Inc., 217 F. Supp. 3d 1116 (N.D. Cal. 2016) (motion to dismiss granted for Twitter as interactive computer service following claims under the Anti-Terrorism Act for death of husbands); Barnes v. Yahoo!, Inc., 570 F.3d 1096 (9th Cir. 2009) (motion to dismiss granted on tort claim of negligent undertaking); Klayman v. Zuckerberg, 753 F.3d 1354 (D.C. Cir. 2014) (motion to dismiss granted in favor of Facebook on tort claims of negligent breach of duty of care and assault after Palestinian death threats to Jews was communicated over Facebook); Doe v. Backpage.com, LLC, 817 F.3d 12 (1st Cir. 2016) (motion to dismiss granted to Backpage.com based on alleged violations of the Trafficking Victims Protection Reauthorization Act).

85. Schruers, *supra* note 36, at 208.

86. *Id.*

seminal cases[87] on the scope of § 230 immunity were decided—both as a result of allegedly discriminatory postings in violation of the Fair Housing Act.[88]

In *Chicago Lawyers' Commission for Civil Rights Under Law, Inc. v. Craigslist, Inc.*, the Seventh Circuit diverged from the Fourth Circuit's broad immunity interpretation of § 230 laid out in *Zeran*. Here, the Chicago Lawyers' Committee for Civil Rights Under the Law sued Craigslist[89] under the Fair Housing Act, alleging Craigslist posted housing ads made by third parties that included discriminatory language, such as "no minorities" and "no children."[90] Referencing its earlier opinion in *Doe v. GTE*, the court found that the interpretation of § 230 is not necessarily "a general prohibition of civil liability for web-site operators."[91] Instead, the court mused "perhaps § 230(c)(1) forecloses any liability that depends on deeming the ISP a 'publisher' . . . while permitting the states to regulate ISPs in their capacity as intermediaries."[92]

That same year, in *Fair Housing Council v. Roommates.com*, the Ninth Circuit found that a website operator, Roommates.com, was unprotected by § 230 because the website had elicited illegal content and made "aggressive use of it in conducting its business."[93] In that case, Roommates.com, a website that helped people to connect with others in hopes of finding a roommate, required its subscribers to select their sex, sexual orientation, and parental status in order to sign up.[94] This information was used to complete the subscriber's profile as well as to help Roommates.com send targeted notifications to subscribers

87. These cases were important not only for their analyses of § 230, but also because they help further define the types of companies that fall under the § 230 definition of "interactive computer service." *See supra* note 13 for a definition of interactive computer services. *See also* 47 U.S.C. § 230(f)(2) (2012); *see also*, Fair Hous. Council v. Roommates.com, LLC, 521 F.3d 1157, 1162 n.6 (9th Cir. 2008) ("Today, the most common interactive computer services are websites.").

88. The Fair Housing Act makes it illegal:

> [t]o make, print, or publish, or cause to be made, printed, or published any notice, statement, or advertisement, with respect to the sale or rental of a dwelling that indicates any preference, limitation, or discrimination based on race, color, religion, sex, handicap, familial status, or national origin, or an intention to make any such preference, limitation, or discrimination.

42 U.S.C. § 3604(c) (2012).

89. Craigslist is a website that "provides an electronic meeting place for those who want to buy, sell or rent housing (and many other goods and services). Chi. Lawyers' Comm. for Civil Rights Under Law, Inc. v. Craigslist, Inc., 519 F.3d 666, 668 (7th Cir. 2008).

90. *Id.*

91. *Id.* at 669; *see also* Doe v. GTE Corp., 347 F.3d 655, 659–60 (7th Cir. 2003) (finding the district court's statutory interpretation—that on one hand, § 230(c)(2) provides immunity when an interactive computer service censors content, while on the other hand, § 230(c)(1) provides immunity when an interactive computer service refrains from censoring content—to be an unlikely legislative intent since this incentivizes interactive computer services to be "indifferent to the content of information they host or transmit."); *see also*, 47 U.S.C. § 230(c)(2) (2012).

92. *Chicago Lawyers*, 519 F.3d at 670 (quoting *GTE Corp.*, 347 F.3d at 660).

93. Fair Hous. Council v. Roommates.com, LLC, 521 F.3d 1157, 1172 (9th Cir. 2008).

94. *Id.* at 1161.

regarding available roommates who are a match.[95] The demographic information was solicited by Roommates.com and by means of dropdown selection menus on its website, completion of which was mandatory, this facilitated users in discriminating against each other, in violation of the Fair Housing Act. In these circumstances, the court held that Roommates.com had forfeited its § 230 immunity by itself becoming an information content provider.[96]

C. Current Congressional Efforts to Amend Section 230

In 2017, in response to widespread coverage and media attention on the series of Backpage.com cases, Congress introduced two bills to amend Section 230 in an effort to provide greater protection for victims of online sex trafficking.[97] Both bills, the Stop Enabling Sex Traffickers Act of 2017 and the Allow States and Victims to Fight Online Sex Trafficking Act of 2017, clarify that § 230 should not be used to shield interactive computer services from criminal and civil liability under the federal human trafficking laws.[98] Taking a fresh look at § 230 immunity, the House version states: "Section 230 of the Communications Act of 1934 (47 U.S.C. [§] 230; commonly known as the 'Communications Decency Act of 1996') was never intended to provide legal protection to websites that facilitate traffickers in advertising the sale of unlawful sex acts with sex trafficking victims."[99] In April 2018, the Allow States and Victims to Fight Online Sex Trafficking Act of 2017 was enacted, adding new language to § 230 clarifying that civil actions brought under criminal sex trafficking laws are not limited or impaired by § 230.[100]

III. AN ANALYSIS OF THE VARIOUS INTERNET LIABILITY APPROACHES

A. Why Strict Liability Failed

The first approach to handling liability for online entities, as seen in the *Stratton Oakmont* era—strict liability[101]—has the benefit of consistent risk allocation, but at the expense of rigidity and with possible chilling effects on innovation and speech. Discussing the evolution of strict liability in industry, Prosser and Keeton write:

> [t]here is a strong and growing tendency, where there is blame on neither side, to ask, in view of the exigencies of social justice, who can

95. *Id.* at 1167.

96. *Id.* at 1170.

97. *Compare* Stop Enabling Sex Traffickers Act of 2017, S. 1693, 115th Cong. (2017) *with* Allow States and Victims to Fight Online Sex Trafficking Act of 2017, H.R. 1865, 115th Cong. (2017).

98. *Id.*; *see generally* 18 U.S.C. § 1591 (2012).

99. H.R. 1865.

100. Pub. L. No. 115-164, 132 Stat. 1254, § 4, Apr 11, 2018 (codified at 47 U.S.C. 230(e)(5)).

101. *See supra* note 55.

> best bear the loss and hence to shift the loss by creating liability where there has been no fault . . . . The courts have tended to lay stress upon the fact that the defendant is acting for his own purposes, and is seeking a benefit or a profit from such activities, and that he is in a better position to administer the unusual risk by passing it on to the public than is the innocent victim. The problem is dealt with as one of allocating a more or less inevitable loss to be charged against a complex and dangerous civilization, and liability is imposed upon the party best able to shoulder it.[102]

Therefore, because interactive computer services and online intermediaries are acting for their own purposes (i.e., benefiting or profiting from the activities on their platforms), and because they are more likely than an individual person to be able to bear the risk, strict liability seems like a fitting solution to the question of who should bear the risk of the inherent dangers of cyberspace.

However, some commentators think public opinion favors the more fault-based negligence standard in tort liability because, ethically, it makes sense to hold someone liable when he or she is at fault. Conversely, in strict liability, an enterprise is held liable even for a no-fault accident.[103] In *Cubby*, the court explained that the First Amendment rights to freedom of speech and press defend interactive computer services from strict liability for unknowingly distributing tortious material over the internet—especially when the interactive computer service had little or no editorial control over the content.[104] Giving credence to this standard, the *Stratton Oakmont* court in turn found the defendant liable because the efforts it made to control and filter its content made it a publisher, not a distributor like Compuserve.[105] Later, the *Zeran* court suggested that holding an interactive computer service liable for the vast amount of content created by third parties on the internet created a strict liability regime.[106] This approach to liability on the internet, the antithesis of Congress's expressed intent for the CDA, would likely have a chilling effect on internet speech.[107]

Essentially, strict liability was rejected because it causes a "Good Samaritan," who is trying to filter or censor obscene content, to be treated as a publisher in the eyes of the law, and thus liable for any harmful remaining content. Congress passed § 230 with the intent of promoting private entity censorship of "objectionable" material on the internet and removing any deterrents from doing

---

102. KEETON ET AL., *supra* note 7, § 75, at 536–37 (internal quotation marks omitted).

103. Henderson, *supra* note 55, at 380, 386. "Only in a limited class of cases, those in which plaintiffs are completely passive victims of risky activities knowingly undertaken by commercial enterprises, are ethical arguments favoring strict liability persuasive." *Id.* at 386.

104. Cubby, Inc. v. Compuserve, Inc., 776 F. Supp. 135, 139–40 (S.D.N.Y. 1991).

105. Stratton Oakmont, Inc. v. Prodigy Servs. Co., No. 31063/94, 1995 N.Y. Misc. LEXIS 229, *9–11 (N.Y. Sup. Ct. May 24, 1995).

106. Schruers, *supra* note 36, at 246; *see also* Zeran v. Am. Online, Inc., 129 F.3d 327, 333 (4th Cir. 1997).

107. *Zeran*, 129 F.3d at 333.

so.[108] Thus, because strict liability creates a conflict with Congress's intent for § 230, it cannot survive as a theory of liability in cyber torts unless § 230 is changed.

B. "The Get-Out-of-Jail-Free Card:"[109] Broad Immunity from Internet Liability

The second approach to § 230, as found in *Zeran*, that Congress intended broad, if not blanket immunity,[110] for interactive computer services, seems to have the most support in American courts since *Zeran*.[111] This is most likely due to the common-sense policy set out in § 230 of furthering the free market on the internet and fostering the advancement of an important technology.[112] Also, *Zeran* assumes that administratively, "[i]t would be impossible for service providers to screen each of their millions of postings for possible problems."[113] Furthermore, this broad immunity approach advances the greatest level of protection of free speech on the internet by reducing service providers' motivation to censor or restrict information provided by third parties; although courts have interpreted the purpose of the CDA's immunity provision to encourage self-regulation.[114]

Although a broadly construed immunity for web operators and internet companies is meant to promote self-regulation by the web industry, it more likely removes the incentive for companies to self-regulate, because § 230 acts like a "get-out-of-jail-free card."[115] This disincentive for interactive computer services to ensure their web products and services are safe should cause concern to consumers.

Although most courts fall in line with *Zeran's* broad approach to the CDA, some have raised questions about it. For example, in *Klayman v. Zuckerberg*, where Facebook was sued for not promptly removing a Palestinian Facebook page that called for Muslims to rise up and kill Jews, the D.C. Circuit considered whether Facebook's failure to remove the content constituted publishing for liability purposes.[116] Although the D.C. Circuit ultimately adopted *Zeran*'s approach, it recognized that publication of tortious material not only means

---

108. *See supra* note 41 and accompanying text.

109. Doe v. Internet Brands, Inc., 824 F.3d 846, 853 (9th Cir. 2016).

110. Andrew M. Sevanian, *Section 230 of the Communications Decency Act: A "Good Samaritan" Law Without the Requirement of Acting as a "Good Samaritan*," 21 UCLA ENT. L. REV. 121, 126 (2014).

111. *See supra* Section I.B.

112. *See supra* note 41 and accompanying text.

113. Zeran v. Am. Online, Inc., 129 F.3d 327, 331 (4th Cir. 1997).

114. *See*, *e.g.*, Schneider v. Amazon.com, Inc., 31 P.3d 37, 41 (Wash. Ct. App. 2001) (explaining Congress chose to protect online intermediaries from liability for harmful third-party content because such immunity would encourage the intermediaries to self-regulate).

115. Doe v. Internet Brands, Inc., 824 F.3d 846, 853 (9th Cir. 2016).

116. Klayman v. Zuckerberg, 753 F.3d 1354, 1358–59 (D.C. Cir. 2014).

communicating that material, but also means *failure to remove* that material.[117] This recognition rekindles a familiar analysis made by the *Stratton Oakmont* court in 1995: where Prodigy held itself out to the public as filtering harmful content from its website, thus exercising editorial control over third-party content, it became liable for any harmful material it failed to remove.[118] Thus, courts dealing with the modern complexities of cyber torts beyond the context of 1990s defamation suits recognize the temptation of applying a strict liability standard, but ultimately tend to feel more comfortable applying the more popular broad immunity approach to § 230 liability.

C. Moving in the Right Direction: Some Standard of Care is Better than None at All

The third approach to § 230, the conditional immunity approach pioneered primarily by the Seventh Circuit in *Chicago Lawyers* and the Ninth Circuit in *Roommates*, is a more even-handed approach because it takes great care to safeguard internet speech, while engaging in the difficult balancing of free market interests with consumer protection.

Recall that, in *Chicago Lawyers*, the Seventh Circuit opened up the door to possible intermediary liability,[119] and in *Roommates*, the defendant website was deprived of § 230 immunity because it was directly involved in developing and making use of certain illegal content on its website and because it profited from it.[120] The Ninth Circuit's condition is this: "If you don't encourage illegal content, or design your website to require users to input illegal content, you will be immune."[121] This seems fair enough and has worked in favor of injured plaintiffs on a few occasions in the context of failure to warn claims.[122] Because "[i]nternet intermediaries often profit directly from transactions that effectively would be banned in an offline environment[,]"[123] keeping a watchful eye out for this behavior and imposing conditional immunity on intermediaries can be an effective way to encourage them to self-regulate more attentively.

The drawback to this approach is that it opens up the door to tort liability for interactive computer services—a result that the *Zeran* court feared would chill

---

117. *Id.*

118. *See* discussion *supra* Section I.B.1.

119. Chi. Lawyers' Comm. for Civil Rights Under Law, Inc. v. Craigslist, Inc., 519 F.3d 666, 669–70 (7th Cir. 2008).

120. Fair Hous. Council v. Roommates.com, LLC, 521 F.3d 1157, 1172 (9th Cir. 2008).

121. *Id.* at 1175; *see also* Anthony v. Yahoo! Inc., 421 F. Supp. 2d 1257, 1262 (N.D. Cal. 2006) (finding an online dating service cannot claim § 230 immunity, when it created false dating profiles, sending them to soon-to-be-expired subscribers to convince them to renew their subscriptions, because it was an information content provider).

122. *See generally* Beckman v. Match.com, LLC, 668 Fed. App'x 759 (9th Cir. 2016); Doe v. Internet Brands, Inc., 824 F.3d 846 (9th Cir. 2016).

123. Mann & Belzley, *supra* note 54, at 247.

internet speech and create prohibitive burdens for interactive computer services.[124]

D. Evaluating the Merits of Non-CDA Liability Regimes: The Negligence[125] or Notice-Liability Approach to Interactive Computer Service Liability[126]

A fourth approach to interactive computer service liability presently does not exist in the United States with respect to interpreting the CDA in cyber tort claims. A negligence or "notice-based" liability regime is, however, prevalent in Europe and modeled in U.S. copyright law under the DMCA.[127] This approach would impose the common law distributor liability upon interactive computer services if they are given notice, or otherwise made aware of the tortious content on their websites or services.[128] In such cases when notice is given, the service provider would have a duty of care to remove the tortious content or otherwise remedy the issue.[129]

1. The European Approach: Imposing a Duty of Care

In 2000, the European Union (EU) passed the Electronic Commerce Directive, which provides rules for EU member countries to adopt regarding e-commerce, communications, and liability for intermediary service providers.[130] The Electronic Commerce Directive creates a duty of care for ISPs—that they should take down tortious materials upon notice.[131]

In a recent case, *Delfi AS v. Estonia*, the Grand Chamber of the European Court of Human Rights agreed with Estonia's Supreme Court that an online news website, Delfi AS, could be held liable for third-party user comments containing threats that were posted on its website.[132] In this case, the Delfi AS

---

124. Zeran v. Am. Online, Inc., 129 F.3d 327, 333 (4th Cir. 1997).

125. "'Negligence' refers to the failure of an actor (including a commercial enterprise) to take reasonable care to prevent harm caused by the actor's conduct." Henderson, *supra* note 55, at 380.

126. Schruers, *supra* note 36, at 232. Schruers describes this approach as distributor liability, "since distributors are held to the same 'knew or should have known' rule commonly applied in negligence regimes." *Id.*

127. *See* Pub. L. No. 105-304, 12 Stat. 2878, § 512, Oct. 28, 1998. Furthermore, the purpose of this section is not to produce an in-depth comparative analysis with European laws, which is not undertaken here; but rather, to use them for illustrative purposes. Similarly, the following discussion on the DMCA is used to illustrate how a notice-takedown regime might operate in the United States.

128. Schruers, *supra* note 36, at 235.

129. *Id.*

130. Rustad & Koenig, *supra* note 2, at 343 n.27.

131. *Id.* at 392–94. Rustad and Koenig offer criticism of the EU's Electronic Commerce Directive on the basis that it is a collection of standards instead of regulations, leaving specific notice-takedown procedures to be legislated by EU member states—an environment that could lead to over-censorship of free expression online. *Id.* at 394 n.304, 407. See *infra* note 131 and accompanying textual material for an illustration of Rustad and Koenig's criticism.

132. Delfi AS v. Estonia, Eur. Ct. H.R., App. No. 64569/09, at 61 (Grand Chamber 2015). This case was brought before the European Court of Human Rights by Delfi AS (a news company

removed the threatening comments upon notice, after approximately six weeks.[133] Although the website allegedly followed the Electronic Commerce Directive's notice and takedown provision, the Grand Chamber affirmed the ruling of the Estonian Supreme Court, finding the website liable as a publisher. In its opinion, the Grand Chamber made a distinction between the duty of care for a commercial news website and that of a less professionally-managed website, such as a social networking site,[134] insinuating that Delfi AS, as a sophisticated player, has a greater obligation to effectively censor hate speech and incitement to violence (neither of which is protected speech in the EU) from its website.[135]

In the United Kingdom, internet service providers have an "innocent dissemination" defense to lawsuits when they can show they were not aware of tortious content.[136] However, to assert this defense requires the defendant company to show it exercised reasonable care in publishing the content at issue.[137] For example, in *Godfrey v. Demon Internet*, a physics professor alleged defamatory content about him was placed online.[138] He forthwith notified the defendant ISP to have it removed, but the ISP did not remove it until two weeks later.[139] The English court ruled that because the defendant ISP was provided with notice, it was unable to use the innocent dissemination defense.[140]

Other European countries that operate under civil law systems take a similar approach. For example, under the German Teleservices Act Section 5, Germany provides for ISP liability for content posted by third parties if the ISP has knowledge of the content and there is a reasonable and feasible way to block it.[141] French civil law requires ISPs to remove objectionable content promptly upon notice—failing to do so could result in liability.[142] To assess liability,

---

registered in Estonia), under the claim that the adverse ruling of the Estonian Supreme Court violated Delfi AS's right to freedom of expression under Article 10 of the European Convention on Human Rights. *Id.* at 3–4. For information on Article 10, *see European Convention on Human Rights, Article 10*, EUROPEAN COURT OF HUMAN RIGHTS COUNCIL OF EUROPE (2010), http://www.echr.coe.int/Documents/Convention_ENG.pdf.

133. Delfi AS v. Estonia, App. No. 64569/09, at 7–8.

134. *Id.* at 8, 45–46.

135. *Id.* at 58–59; *see generally id.* for discussion and analysis concerning publisher versus intermediary liability in the European context.

136. Schruers, *supra* note 36, at 227.

137. *Id.*

138. *Id.*

139. *Id.*

140. *Id.*

141. *Id.* at 228; *see also* Act on the Utilization of Teleservices (Gesetz über die Nutzung von Telediensten), 1997 (Ger.), https://germanlawarchive.iuscomp.org/?p=694#5.

142. Schruers, *supra* note 36, at 230.

French courts focus on the conduct of the ISP after notice of tortious material is given.[143]

2. The DMCA: Paving the Way for Notice-Based Liability on the Internet

Enacted into law in the United States in 1998, the DMCA also creates a notice-based liability regime for online service providers, limited to the realm of copyright infringement.[144] In part, "[t]he DMCA was enacted to strike a new balance between the viable operations of OSP's [online service providers[145]] and the need to enforce copyright protection."[146] Its "immunity" provision protects service providers from monetary liability due to third-party copyright violations as long as (1) the service provider is unaware of the alleged copyright infringement on its website or service and (2) the service provider adheres to the "take down" provision by promptly, upon notice, removing or blocking access to the allegedly infringing material.[147] Moreover, because the burden is on the complaining party to give notice, a service provider is not required to actively monitor its website or internet service for copyright violations.[148]

The negligence or notice-based approach espoused in Europe and utilized in the DMCA, has the benefit of providing a clear "reasonable" standard of care for companies to follow, while providing an innocent dissemination defense to help protect companies. Moreover, applying a notice-takedown approach to cyber tort liability has the benefit of

---

143. Xavier Amadei, Note, *Standards of Liability for Internet Service Providers: A Comparative Study of France and the United States with A Specific Focus on Copyright, Defamation, and Illicit Content*, 35 CORNELL INT'L L.J. 189, 197 (2002).

144. Schruers, *supra* note 36, at 236.

145. "'[S]ervice provider' means an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received." Pub. L. No. 105-304, 12 Stat. 2878, § 512, Oct. 28, 1998.

146. § 512, 12 Stat. at 2878; Costar Grp., Inc. v. Loopnet, Inc., 164 F. Supp. 2d 688, 698 (D. Md. 2001).

147. § 512, 12 Stat. at 2878; *Costar Grp.*,164 F. Supp. 2d at 698; *see also* ALS Scan, Inc. v. RemarQ Cmtys., Inc., 239 F.3d 619, 625 (4th Cir. 2001) ("The DMCA was enacted both to preserve copyright enforcement on the Internet and to provide immunity to service providers from copyright infringement liability for 'passive,' 'automatic' actions in which a service provider's system engages through a technological process initiated by another without the knowledge of the service provider. This immunity, however, is not presumptive, but granted only to 'innocent' service providers who can prove they do not have actual or constructive knowledge of the infringement, as defined under any of the three prongs of 17 U.S.C. § 512(c)(1). The DMCA's protection of an innocent service provider disappears at the moment the service provider loses its innocence, i.e., at the moment it becomes aware that a third party is using its system to infringe. At that point, the Act shifts responsibility to the service provider to disable the infringing matter, 'preserving the strong incentives for service providers and copyright owners to cooperate to detect and deal with copyright infringements that take place in the digital networked environment.'" (citations omitted)).

148. Donald P. Harris, *Time to Reboot?: DMCA 2.0*, 47 ARIZ. ST. L.J. 801, 803–04 (2015).

> harmoniz[ing] elements from the common law of distributor liability, the [DMCA's] . . . notice-and-takedown procedure, and the European Union's E-Commerce Directive . . . . [And, it might] jumpstart the field of cybertorts so that it can develop into an effective social control mechanism for cyberspace.[149]

Furthermore, in U.S. common law, a negligence (fault-based) approach to tort liability is supported in tradition and seen as fairer than a strict liability.[150] Negligence-based liability rationally has more focused deterrence value than strict liability and achieves "a substantial measure of loss distribution."[151]

Finally, the DMCA regime does what the CDA fails to do: it saves interactive computer services from the prohibitive expenses of web content monitoring by shifting the burden to the complaining party to give initial notice of objectionable material, and in doing so, it gives the consumer a clear-cut way to begin the process of mitigating the harm being caused.[152] This provides protection for ISPs against "uncertain and crippling damages, which would curtail the development of the [i]nternet[,] . . . encouraging the continued expansion and development of the [i]nternet"[153]—in large part, the same policy result contemplated by the CDA.[154]

The problems with the negligence or notice-based approach, however, are manifold. First, it can drain companies' coffers by enabling frivolous suits of the kind warned about in *Zeran*, encouraging companies to settle to save money on litigation.[155] Second, it could encourage service providers to over censor information on the internet as a way of avoiding notice-based liability and costs associated with handling notice and takedown procedures.[156] Furthermore, it might encourage companies to go overseas to find more favorable laws.[157] Finally, it might increase extortion by lawsuit, creating a *de facto* injunction on

149. Rustad & Koenig, *supra* note 2, at 343–44. Rustad and Koenig argue that by removing the broad immunity protections of § 230 from ISPs and implementing a cybertort notice-takedown policy, tort law will catalyze further legal reform (as it historically has done in other arenas), which will increase consumer protection on the internet. *Id.*

150. Henderson, *supra* note 55, at 386.

151. Henderson, *supra* note 55, at 380, 386; *see also*, Gary T. Schwartz, *The Beginning and the Possible End of the Rise of Modern American Tort Law*, 26 GA. L. REV. 601, 636 (1992) (explaining some tort law scholars, such as Prosser and Keeton, view moral responsibility, not loss distribution, to be the proper aim of tort liability).

152. *Cf.* Zeran v. Am. Online, Inc., 129 F.3d 327, 333 (4th Cir. 1997) (imagining the "impossible burden" of monitoring all transmissions and making judgment calls on each potentially objectionable piece of information that an interactive computer service would face in a notice-liability regime).

153. Harris, *supra* note 147, at 803–04.

154. *See supra* note 41 and accompanying text.

155. *Zeran*, 129 F.3d at 333; *see also* Schruers, *supra* note 36, at 228.

156. *Zeran*, 129 F.3d at 333.

157. Schruers, *supra* note 36, at 229.

internet content every time a person might feel offended by something.[158] In economic terms, this might "externalize liability costs, transforming them into social costs by allowing [offended or otherwise] self-interested plaintiffs to control the content of public discourse."[159]

IV. MODERNIZING THE CDA

A. Internet Liability Will No Longer Stifle Technological Growth

With such rudimentary knowledge of the future growth and impact of the internet, Congress showed great foresight when it attached the Good Samaritan provision to § 230 of the CDA in 1996. Allowing the fear of internet indecency to lead internet policy back in 1996, while leaving interactive computer services overly exposed to liability, could have crippled Silicon Valley's innovation and global leadership in the technology sector.

However, at the time of this writing, 23 years have passed since the CDA was enacted into law. We now know that the internet is fundamentally different from telegraphs, telephones, and radiotelegraphs; and internet crime, abuse, and harassment takes "[o]bscene or harassing phone calls" to a whole new level.[160] Moreover, tech innovation and the free market on the internet are arguably no longer in danger of being stifled in their incipiency.[161] According to the Ninth Circuit:

> The [i]nternet is no longer a fragile new means of communication that could easily be smothered in the cradle by overzealous enforcement of

158. *Id.* at 244; *see also Zeran*, 129 F.3d. at 333.

159. Schruers, *supra* note 36, at 244. An externality is defined as "[a] consequence or side effect of one's economic activity, causing another to benefit without paying or to suffer without compensation." *Externality*, BLACK'S LAW DICTIONARY (10th ed. 2014).

160. *See* Cannon, *supra* note 33, at 53, 57, 73–75 (discussing how the CDA was conceivably based on an assumption that the internet is analogous to other commonly regulated telecommunications devices, such as telephones, and should therefore be similarly regulated for decency); *Compare* 47 U.S.C. § 223 (2000) (Title 47 is named "Telegraphs, Telephones, and Radiotelegraphs"), *with* 47 U.S.C. § 223 (2012) (Title 47 is renamed "Telecommunications"); *see also supra* Section I.A. For an in-depth description of the contours of the internet as understood by the judiciary, *see generally* Reno v. A.C.L.U., 521 U.S. 844, at 849–57 (1997).

161. *See* Citron & Wittes, *supra* note 8, at 422 ("'The law's reaction to claims against such large actors for new types of harms typically goes through' distinct phases. Law first recognizes the new form of harm but not the benefit that the new technology has occasioned. This drives it to adapt existing theories of liability to reach that harm. After the technology's benefits become apparent, law then reverses course, seeing its earlier awards of liability as threats to technological progress and granting sweeping protection to the firms in the new industry. Once the technology becomes better established, law recognizes that not all liability awards threaten its survival. Law then separates activities that are indispensable to the pursuit of the new industry from behavior that causes unnecessary harm to third parties. This is what the celebrated *Palsgraf v. Long Island Railroad Co.* case accomplished and much of the reason the negligence standard emerged. As the new technology becomes more familiar, law refines the distinction between acceptable and unacceptable harms, at times setting liability rules to drive the development of less destructive means of carrying out the necessary functions.").

> laws and regulations applicable to brick-and-mortar businesses. Rather, it has become a dominant—perhaps a preeminent—means through which commerce is conducted. And its vast reach into the lives of millions is exactly why we must be careful not to exceed the scope of immunity provided by Congress . . . .[162]

"[Moreover,] [t]he Communications Decency Act was not meant to create a lawless no-man's-land on the [i]nternet."[163] These insights are important to consider as internet technology continues to grow, pervading the personal lives of almost everyone and connecting us to countless potential sources of harm. In a disturbing, but predictable, turn of events, the internet has become one of the most effective and efficient ways to commit crime[164] and engage in often anonymous, harmful, anti-social behavior.[165]

Thus, Congress should modernize its internet policy in favor of a more well-balanced free market and consumer protection analysis and amend § 230 accordingly. Because internet regulation could prove harmful to innovation, driving American technology companies to incorporate overseas, the common-sense solution is to amend § 230 to include a notice-based harmful content removal provision similar to that of the DMCA, which is more in line with European doctrine.[166] Having a harmonious approach to liability on the internet across the West could help bring consistency across borders, mitigating incentives for online intermediaries to incorporate overseas.[167]

B. A Call to Amend § 230: Removing Good Samaritan Protection from Bad Samaritans

Some commentators have suggested analytical workarounds for § 230 immunity. For example, one commentator suggests the ridesharing service Uber should not be given § 230 immunity because it sets prices on its ridesharing application, making it an information content provider.[168] Other commentators point out the inevitability of government regulation of the internet and suggest regulatory solutions,[169] while others propose different variations of the aforementioned liability schemes.[170] However, because Congress recently

---

162. Fair Hous. Council v. Roommates.com, LLC, 521 F.3d 1157, 1165 n.15 (9th Cir. 2008).

163. *Id.* at 1164.

164. Europol, Internet Organized Crime Threat Assessment 2017, (2017) https://www.europol.europa.eu/sites/default/files/documents/iocta.pdf. (discussing cyber-dependent crimes such as malware, critical infrastructure attacks, and data breaches as well as online financial crime, sexual exploitation of children, proliferation of terrorist ideologies, and tampering with democratic elections).

165. *See supra* notes 5, 21, 84 and accompanying text.

166. *See* Rustad & Koenig, *supra* note 2, at 407–08.

167. *See generally id.* at 343.

168. Allen, *supra* note 72, at 318. Under § 230, an information content provider itself is not immune from liability. *See supra* note 15 and accompanying text.

169. *See* Mann & Belzley, *supra* note 54, at 250.

170. *See* Rustad & Koenig, *supra* note 2, at 343.

amended § 230 to ensure facilitators of online sex trafficking cannot hide behind its immunity provision,[171] now is a crucial time to re-evaluate these solutions to internet abuse and overbroad application of § 230 immunity.

Interactive computer services should not retain the broad immunity available under the current majority interpretation of § 230, but should instead be reachable via tort actions when victims can show there was negligence or a failure to warn.[172] Thus, the scope of § 230 immunity should be amended to clarify that broad immunity should no longer be the default approach. Rather, § 230 should be expanded beyond the context of the 1990s focus on publishing, defamation, and Good Samaritan filtering of pornography, to clarify that interactive computer service action or inaction falling within the realm of *facilitation*, *gross negligence*, *willful ignorance*, or *recklessness* should not be protected, despite the fact that a third-party is the source of the harmful content or activity.[173] While the April 2018 amendment was a necessary and constructive step for updating § 230, it was not broad enough as to establish a standard of care applicable to other harms beyond the facilitation of sex trafficking.

In support of creating this reasonable standard of care for interactive computer services, there should be a formalized notice-based takedown procedure in place to give consumers a self-defense option against harmful content or mechanisms and to encourage identification and reporting of various abuses, such as incitement to violence, bullying, revenge porn, fraudulent schemes, criminal enterprises, and foreign meddling. Although some might argue this approach to liability will burden interactive computer services due to frivolous litigation, this approach is the most balanced approach available. It gives consumers a reasonable measure of protection, shifting the burden to them to report problems, without increasing the burden on interactive computer services by implementing a formalized regulatory approach.[174]

Furthermore, Congress should re-evaluate § 230 for applicability to the modern-day internet reality. In drafting § 230, Congress made the effort to lay out five "findings" regarding the great potential and utility of the internet[175]

---

171. *See supra* notes 5, 22, 102 and accompanying text.

172. *See generally* Tarasoff v. Regents of Univ. of California, 551 P.2d 334 (Cal. 1976).

173. *See generally* KEETON ET AL., *supra* note 7, §§ 34, 53, at 208–14, 359.

174. Self-regulation of the internet industry through notice and takedown and litigation will continue to encourage Silicon Valley to do what it does best—innovate. Creating a standard of care for interactive computer services to adhere to should encourage positive citizenship in the form of forcing the industry to address the problem of consumer safety with high-tech solutions.

175. Congress stated:

> (a) Findings.—The Congress finds the following:
>
> (1) The rapidly developing array of [i]nternet and other interactive computer services available to individual Americans represent an extraordinary advance in the availability of educational and informational resources to our citizens.

along with five policy points (seeking to protect the growth of the internet in its incipiency);[176] yet, in enacting the CDA, Congress failed to lay out findings or policy in the Act pertaining to the potential dangers of the internet beyond obscenity, stalking, and harassment.

From the text of the statute itself, as well as from its legislative history, the CDA was introduced primarily to combat internet pornography.[177] But what the CDA lacks overall is a comprehensive policy discussion analyzing some of the other consequences and dangers of a free and open internet sans any incentive for civilized and responsible behavior. This is a task that Congress should undertake in re-evaluating the CDA and § 230 immunity.

Thus, in addition to the Allow States and Victims to Fight Online Sex Trafficking Act of 2017), Congress should amend § 230 to clarify that upon notice of harmful activity occurring via a website, the responsible interactive service provider would breach its reasonable duty of care by ignoring an active illicit enterprise or course of conduct that is harming people, as discussed above.[178]

In drafting the Allow States and Victims to Fight Online Sex Trafficking Act of 2017, Congress explicitly recognized that they never intended § 230 to immunize interactive computer services that facilitate bad acts, specifically the advertising of sex trafficking victims.[179] This opens the door to questions of what other kinds of bad actors Congress did not intend § 230 to provide immunity to[180]—questions of which Congress needs to provide an answer.

V. CONCLUSION

According to Mann and Belzley:

> The pirates have arrived on the high seas of the online world and the lack of regulation makes their predations all too easy. The time has

---

> (2) These services offer users a great degree of control over the information that they receive, as well as the potential for even greater control in the future as technology develops.
>
> (3) The [i]nternet and other interactive computer services offer a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity.
>
> (4) The [i]nternet and other interactive computer services have flourished, to the benefit of all Americans, with a minimum of government regulation.
>
> (5) Increasingly Americans are relying on interactive media for a variety of political, educational, cultural, and entertainment services.

Pub. L. No. 104-104, 110 Stat. 137–38, § 509, Feb. 8, 1996.

176. *See supra* note 41 and accompanying text.

177. *See* § 502, 110 Stat. at 133; H.R. REP. NO. 104-458, at 187–90 (1996) (Conf. Rep.).

178. *See* Rustad & Koenig, *supra* note 2, at 408.

179. *See supra* note 22.

180. For example: cyberbullies and revenge pornographers, people who incite violence and terrorism, sexual predators, child pornographers, fraudsters, and foreign intelligence organizations.

> come for lawmakers to implement sensible policies designed to reign in the pirates while minimizing the impact on law-abiding [i]nternet users.[181]

For several years, § 230 successfully protected the growth of internet-based technology and innovative communication methods while guarding free speech on the internet. However, the internet industry is now on solid footing and freedom of speech remains firmly intact. In the modern internet era, where connection to the internet pervades the lives of anyone with a smartphone, dangers have grown.[182] Leaving internet self-regulation up to the discretion of companies accountable to investors and profits is no longer a prudent course.

As a result of § 230, many victims of internet-related crime, abuse, and harassment have been left without meaningful recourse in tort law. Congress should therefore amend § 230 to include a notice-based takedown procedure as outlined above, which would hold interactive computer services liable for failing to comply with the procedure. Moreover, interactive computer services should not be given broad immunity, but should be held to a reasonable standard of care in negligence. In a society where individuals have no choice but to interact, learn, and do business online, it makes no sense that tort law causes of action should be practically impossible to sustain for those who are harmed online. Congress must modernize this country's internet policy to protect consumers in cyberspace more robustly and deter antisocial and tortious activity more vigorously.

181. Mann & Belzley, *supra* note 54, at 306.

182. *Id.*